REPÚBLICA DEL ECUADOR

UNIVERSIDAD TECNOLÓGICA EMPRESARIAL DE GUAYAQUIL

TRABAJO DE GRADO
PARA LA OBTENCIÓN AL TITULO DE:

Ingeniería en Sistemas Computacionales Mención Aplicaciones Web y Multimedia

TEMA:

ANÁLISIS DE VULNERABILIDADES A NIVEL DE SEGURIDAD INFORMÁTICA EN EL PARQUE COMPUTACIONAL DE AGUAPEN EP EN EL 2016

AUTOR:

WILLIAM MARCELO RODRÍGUEZ PLAZA

TUTOR:

MSc. VÍCTOR FERNÁNDEZ

OCTUBRE 2016

GUAYAQUIL ECUADOR

DECLARACIÓN EXPRESA

Yo, William Marcelo Rodríguez Plaza, con cédula de ciudadanía No. 0913912762, declaro bajo juramento que la tesis aquí escrita es de mi autoría, y las referencias bibliográficas son consultas, que se incluyen en este escrito.

Renuncio a todos los derechos de autor de la presente tesis de grado, y los actuales derechos de autor pasan a ser propiedad de la Universidad Tecnológica Empresarial de Guayaquil. Según lo establece la ley de Propiedad Intelectual, en su reglamento y normativa vigente.

William Marcelo Rodríguez Plaza

c.c.0913912762

CERTIFICADO DEL TUTOR

Certifico que el presente trabajo de tesis fue desarrollado por William Marcelo Rodríguez Plaza, bajo mi supervisión.

CERTIFICADO DEL TRIBUNAL

Certifico que el presente trabajo de tesis de William Marcelo Rodríguez Plaza, fue calificado por el tribunal.

DEDICATORIA

Dedico mi tesis primeramente a Dios, por sus bendiciones y cuidado, ya que sin Él no lo hubiera logrado terminar mi carrera profesional.

A mis padres por su apoyo incondicional y ayuda desinteresada en las etapas de mi vida.

A mis hijos que con su cariño y compañía que han sido una fuente de alegría y motivación.

AGRADECIMIENTO

A la Universidad Tecnológica Empresarial de Guayaquil, que tuvo el acierto de ofrecer carreras de Sistemas en modalidad semi presencial, a todos los directivos que han sabido guiar en el proceso de pre grado.

A los profesores, que, con paciencia, mística y sabiduría me ayudaron a obtener los conocimientos necesarios para mi profesión.

Especialmente agradezco a mi tutor de tesis por ayuda y guía para lograr terminar mi tesis.

También agradezco a la unidad de observación, la empresa pública AGUAPEN EP, por permitirme hacer uso de sus instalaciones.

RESUMEN

En el presente estudio se procura conocer ¿cuáles son los problemas de seguridad informática, que tiene la empresa pública Aguapen EP en el año 2016 y su incidencia en la perdida de producción en los usuarios del parque de computadoras de esta institución?

Mediante la investigación de las herramientas tecnológicas para la seguridad informática, determinar la mejor solución a implementarse para incrementar la seguridad informática en las computadoras de esta empresa pública.

A partir de esta investigación se establecen conclusiones sobre cuál es la mejor herramienta tecnológica de seguridad informática para empresas, tomando en cuenta la relación costo – beneficio para la empresa.

El objetivo es implementar la mejor solución para salvaguardar los datos, equipos de computación y la producción de la empresa pública Aguapen EP de la ciudad de Salinas en el año 2016.

Para que este objetivo se cumpla, se va a hacer uso de la epistemología de la Investigación Empirista. El diseño de la investigación, es, no experimental – transaccional. El tipo de investigación es descriptiva, El método de investigación que se va a usar es, el método Hipotético – Deductivo, porque, se plantea una hipótesis y se elabora una encuesta. La encuesta se plantea, para observar los resultados obtenidos, y estos resultados ayudaran en la comprobación de la hipótesis.

Palabras claves

Estudio	Informática	Seguridad
Tecnología	Computadora	Institución

ABSTRACT

In the present study seeks to know what are the problems of security, which has Aguapen EP public company in 2016 and its impact on the loss of production in park users of computers of this institution are?

Through research of technological tools for computer security, determine the best solution to be implemented to increase security on computers of this public company.

From this research findings on how best technological tool for computer security undertakings, taking into account the cost - benefit to the company.

The aim is to implement the best solution to safeguard data, computer equipment and production of the public company Aguapen EP city of Salinas in 2016.

For this objective is met, it will make use of the empiricist epistemology of Research. The research design is not experimental - transactional. The research is descriptive, the research method to be used is the hypothetic - deductive method, because a hypothesis is proposed and a survey is made. The survey is proposed to observe the results, and these results help in testing the hypothesis.

Key Words

Study	Computing	Security
Technology	Computer	Institution

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El Profesor Leonard Adleman en 1984, utilizó en una conversación con Fred Cohen por primera vez el término “virus informático”, para referirse a un programa de ordenador que se puede copiar a sí mismo.

Un virus es un malware que puede alterar el funcionamiento de un computador sin el permiso del usuario. El mismo tiene como función, propagarse a través de un software. Su nombre se debe, porque tiene el mismo comportamiento de un virus biológico.

Una de las características de los virus, es el consumo de los recursos de la computadora, por ende, producen pérdida de productividad, cortes en los sistemas de información y daños a nivel de los datos.

Otra característica es su poder de propagación por medio de réplicas o copias, muchas veces utilizan redes de computadoras que no tienen una seguridad adecuada y por ende son vulnerables. Los virus también son usados para ataques de hackers, para causar daño a las computadoras, robo de información y hurto de capitales en efectivo a personas y empresas.

El virus informático ataca los diferentes sistemas operativos que existen en la empresa pública Aguapen EP, como Windows, Linux y Mac. En computadoras, servidores y dispositivos móviles.

Es necesario implementar una herramienta tecnológica para empresas, con seguridad Endpoint, para encontrar el malware más reciente, con acceso a un monitoreo centralizado y seguridad informática asistida en la nube, para estar un paso más adelante que los hackers.

Esto evidencia la importancia de implementar las buenas prácticas de seguridad informática en toda empresa, y para que este objetivo se cumpla, se debe hacer uso de herramientas tecnológicas empresariales, en seguridad informática, para la prevención, detección y reparación de

los ataques a la seguridad informática, por personas internas o externas, a la empresa. Los casos de éxito aumentan con un monitoreo continuo a las computadoras y sus seguridades.

Según los estudios realizados, a la seguridad informática en las empresas, un rango importante de los ataques a la seguridad informática, en las computadoras, de las empresas, a nivel mundial, son dirigidos por personal, de la misma empresa, por oscuros motivos personales, contra la empresa, en la que trabajan, para ocasionar daños en las computadoras, por el descontento contra la empresa. Por ende, es necesario el uso de las normas, políticas, reglas y herramientas a la seguridad informática en toda empresa, para salvaguardar la integridad de la información y los equipos de computación.

CAPITULO I

1 El Problema

Encontrar los problemas de seguridad informática en el parque de computadoras de la empresa Aguapen EP, con las herramientas tecnológicas más adecuadas y eficientes para la prevención, detección y reparación de problemas de seguridad informática, como infección por virus, malware y ataques de hackers, en la empresa AGUAPEN EP.

1.1 Antecedentes

Con el objetivo de neutralizar toda amenaza de virus en la empresa Publica Aguapen EP, se debe implementar una solución con el uso de herramientas tecnológicas en seguridad informática. Para la prevención, detección y corrección de infecciones de virus informáticos.

Actualmente los virus informáticos atacan a todos los sistemas operativos conocidos, desde una computadora con Windows hasta un teléfono celular con su sistema operativo Android, también se incluyes los sistemas operativos más robustos como Unix y Linux. Igualmente se ha desarrollado virus multiplataforma, que pueden infectar varios tipos de sistemas operativos a la vez. Aumentando su nivel de peligrosidad para las computadoras y la información que en ellas se guarda.

En el texto de la revista, Tecnología y Sociedad, se lee: "*Qué tipo De virus esconde las páginas de la Deep Web*"

> **[…] "un virus informático tiene como objetivo alterar el funcionamiento de una computadora, sin el permiso del usuario. Por lo general estos virus, suelen reemplazar archivos ejecutables del sistema por otros infectados con la intención de modificarlos para destruirlos de manera intencionada".** (Condar Guisbert, 2014)

El autor mediante su escrito se enfoca en la definición de un virus, y podemos analizar el alcance del potencial destructivo que tiene un virus informático. Sumado esto a la existencia de más de 10.000 virus

informáticos en el mundo, las posibilidades de infección de un virus informático en una computadora sin protección en seguridad informática, son muy altas.

Los virus informáticos son una amenaza para toda computadora que no tenga una protección adecuada y eficaz, estos programas maliciosos están programados para reproducirse y propagarse por programas infectados, redes de computadora e internet.

En la revista científica, Ciberseguridad, Seguridad de la Información y Privacidad, se lee: "*¿Qué sabemos acerca del web malware?"*

> **[…] "El web malware es aquel código malicioso que es ejecutado por el ordenador de la víctima al acceder a web dañinas. El método por el cual se consigue este resultado se basa principalmente en el aprovechamiento de vulnerabilidades o deficiencias en las configuraciones de seguridad en todo el software relacionado con la navegación web".** (Grácia, 2013)

Como se lee, en la cita anterior los métodos para infectar computadoras con malware, se perfeccionan cada día, los atacantes están continuamente buscando vulnerabilidades en las configuraciones de seguridad en el software que usamos para navegar en internet, este hecho cotidiano puede exponer a un sin número de peligros de seguridad informática, cuando una computadora no tiene instalas y configuradas, herramientas tecnológicas de seguridad informática. La computación por ser una ciencia abstracta, no podemos saber de forma empírica, cuando nuestro ordenador está siendo atacada por piratas cibernéticos o malware, los resultados los vemos después, que se ejecutó el ataque, de robo de información, daño de datos, daño en el hardware, etc.

Toda computadora debe estar protegida por herramientas tecnológicas en seguridad en informática, en especial donde hay una alta concentración de equipos de computación y usuarios, como son las empresas públicas y privadas.

En la tesis de Masterado, se lee: "*Malware en Android, con medidas de prevención*"

> […] "En este trabajo se hace un estudio en profundidad sobre la situación actual de la plataforma Android focalizándolo en la seguridad. A continuación, se analiza, de forma general, el malware en Android". (Villanova-Pascual, 2016)

Como se expresa en la cita anterior, el autor hace un énfasis a la seguridad de dispositivos móviles con sistema operativo Android, actualmente este tipo de seguridad se llama, seguridad de endpoints, y se toma a consideración los dispositivos móviles, porque tienen fallas de seguridad informática, donde los hackers pueden explotar estas fallas, haciendo vulnerables a los dispositivos móviles, ya sean teléfonos inteligentes o tables, y por este medio los hackers tienen la forma de transmitir virus a las computadoras de los usuarios cuando se conectan a sus dispositivos móviles. Esta nueva forma de contagio actualmente se explota por los hackers, y les permite infectar virus que atentan a la privacidad del usuario, virus para dañar la información.

En la tesis de Masterado, se lee: "C*aso de estudio de la Amenaza "Octubre Rojo"* "

> **[…] "La necesidad de adaptar la seguridad de las comunicaciones y los sistemas de información a la realidad de la evolución continua de las amenazas y la sofisticación de los ataques, ha forzado la aparición de una nueva disciplina denominada Ciberdefensa".** (Abad-Aramburu, 2015)

Como podemos leer en la cita anterior, aparece una nueva disciplina llamada Ciberdefensa, sumada a la disciplina Ciberseguridad, las que estudian la forma de defensa a la privacidad y evitar perdida de información de los usuarios con herramientas tecnológicas de seguridad informática con carácter proactivo, la seguridad informática es muy importante en todos equipo o dispositivo que maneje información de los usuarios o critica, porque con buenas practicas, estándares, protocolos, métodos, reglas, herramientas y leyes se minimiza los posibles riesgos de ataques malintencionados por parte de terceras personas a la infraestructura y la información de empresas y usuarios. Aplicando todos

estos conceptos de seguridad informática se consigue sistemas de información seguros y confiables.

1.2 Justificación

Es importante la prevención, detección y reparación de las amenazas a la seguridad informática por virus y considerando el incremento de infecciones de virus informáticos en el parque de computadoras de la empresa Aguapen EP. Por ende, surge la necesidad de salvaguardar la información de la empresa, y sus equipos de computación, mediante el uso de herramientas tecnológicas de seguridad informática, de última generación.

La relevancia de la seguridad informática es monitorear en tiempo real lo que pasa a cada computadora, con el uso de herramientas tecnológicas de seguridad informática para empresas, con el objetivo de encontrar de forma proactiva fallos de seguridad en cada computadora, de esta forma se puede anticipar a encontrar una solución inmediatamente, antes que cause daño los problemas detectados en seguridad informática.

La novedad de estas herramientas tecnológicas de seguridad informática es tener la asistencia tecnológica, desde la nube en tiempo real, para solucionar problemas de seguridad informática, en menos de un segundo de tiempo.

1.3 Campo de estudio

El campo de estudio es la Seguridad Informática, las Tics y la Computación.

La seguridad informática cuida del activo más importante de una empresa, es la información, por ende, deben existir técnicas y procesos que la aseguren, incluyendo la protección a los equipos que almacenan la

información de la empresa, estas defensas dan una seguridad lógica que consiste en la implementación de muros de fuego e instrucciones que resguardan la integridad de los datos, de la empresa y solo se permite el acceso a la información a las personas autorizadas para hacerlo.

Las Tics significan, Las tecnologías de la Información y la Comunicación. Esta tecnología se encarga de gestionar y planificar los conceptos computacionales de los equipos de cómputo y de las habilidades del personal que maneja las computadoras. Esta tecnología abarca los sistemas de redes de computadoras, el software, el hardware, la seguridad y la eficiencia en el uso de estos recursos computacionales. Con la aparición del internet se intensificó el uso de las Tecnología de la Información, al brindar aplicaciones distribuidas de uso general y el proceso de datos en la nube

La Computación abarca las ciencias de la información y la computación y su aplicación en los sistemas computacionales. Es el estudio sistemático de los procesos algorítmicos que analizan y transforman la información, mediante su análisis, diseño, implementación y aplicación de procesos computacionales. La computación esta relaciona con la cuantificación de la información y sus procesos para transformar los datos, de aquí radica la pregunta fundamental en las ciencias de la computación ¿Qué puede ser eficientemente automatizado? Esta pregunta está enfocada a la información que puede ser computada y la cantidad de recursos que se deben usar para ejecutar la computación de la información con sistemas computacionales

1.4 Planteamiento del problema

Los virus informáticos han infectado muchas computadoras desde que fueron creados, produciendo daño en los datos y en los equipos de computación de las empresas públicas y privadas. Esto ha repercutido en pérdida de producción de las empresas. Sumando por millones de dólares los daños ocasionados a nivel mundial.

La empresa pública Aguapen EP, no puede detener su producción de potabilización de agua, incluyendo su distribución. Porque cien mil personas en la provincia de Santa Elena se quedarían sin el líquido vital, ocasionando grandes pérdidas económicas para la empresa, así también para las personas que viven en la provincia, afectando al comercio, a la industria y el turismo.

Es de suma importancia salvaguardar los datos y equipos de computación de la empresa AGUAPEN EP, de amenazas de ataques de virus, porque la empresa tiene toda información de la gestión de facturación, gestión de cobranza, producción, control administrativo y financiero, en sus computadoras.

La solución de seguridad informática de tipo empresarial, debe ser la más versátil para controlar las firmas del software, análisis heurístico y de comportamiento, protección asistida desde la nube y el sistema de prevención de intrusión basado en host con firewall personal. Buscando un punto de equilibrio en la relación costo – beneficio para la empresa.

1.5 Formulación del problema

¿Qué herramienta empresarial tecnológica de seguridad informática, puede solucionar problemas de vulnerabilidades, en la seguridad informática de la empresa pública AGUAPEN EP?

1.6 Sistematización del problema

a) Fase teórica

   ¿Qué son los problemas de vulnerabilidades a la seguridad informática?

b) Fase metodológica

¿Cuáles son las mejores herramientas tecnológicas de seguridad informática, para corregir vulnerabilidades de seguridad informática en la empresa Aguapen EP?

c) Fase de análisis de resultados

¿Qué amenazas en seguridad informática fueron detectas en la empresa Aguapen EP en el año 2016?

d) Fase de la propuesta

¿Qué herramienta tecnológica es más conveniente, usar para controlar la seguridad informática en la empresa Aguapen EP?

1.7 Objetivos de la investigación

1.7.1 Objetivo general

Establecer la mejor herramienta de seguridad informática que se ajuste a las características del parque de computadoras de la empresa pública Aguapen EP en el año 2016

1.7.2 Objetivos específicos

- Determinar los principales tipos, de problemas de seguridad informática existentes a nivel mundial u otros escenarios.
- Investigar cuales son las mejores herramientas tecnológicas para la seguridad informática
- Determinar que amenazas a la seguridad informática, se encuentran en la empresa Aguapen EP en el año 2016
- Sugerir una solución a los problemas de seguridad de los datos y computadoras, usando herramientas tecnológicas para la seguridad informática en la empresa pública Aguapen EP

CAPITULO II

2. El Marco Teórico

En este capítulo se muestra los conceptos básicos de la seguridad informática, que se aplican para salvaguardar la integridad y disponibilidad de la información. En la actualidad la información es considerada, el activo fijo intangible más valioso que tiene una empresa, y como tal se le debe asignar los recursos necesarios para la instalación e implementación de las herramientas tecnológicas de seguridad informática. Con un continuo monitoreo al uso de los equipos de computación y su software.

La ciencia a utilizar es la ingeniería de Sistemas, con un enfoque a la implementación de la seguridad informática, debido al incremento de tecnologías en las ciencias de la computación, creció el tipo y número de ataques a las vulnerabilidades de los equipos

2.1 Ciencia

La ciencia a utilizar es la Ingeniería en Sistemas Computacionales, la cual estudia el desarrollo de los sistemas computacionales y el uso de los lenguajes de programación enfocándose al análisis, diseño y la implementación del hardware y software para desarrollar las más avanzadas aplicaciones telemáticas.

En la revista científica, Ciencia e Ingeniería Neogranadina, se lee: "*Las matemáticas en la ingeniería a través de la historia*"

> […] "En la tecnología, las matemáticas también tienen su aporte principalmente en la computación que da un fuerte empuje a las comunicaciones, las cuales avanzan a diario". (De Alonso, 2016)

Como expresa el texto anterior, la Ingeniería de Sistemas tiene un apoyo fundamental en la ciencia exacta de la matemática, para el desarrollo de los algoritmos de programación, donde se incluye expresiones algebraicas para simplificar los procesos de diseño y elaboración de los

programas y aplicaciones, las matemáticas permiten realizar cálculos algebraicos en el proceso de la información.

Las ciencias de la matemática también ayudan, en los cálculos en las comunicaciones de las redes de corto y largo alcance en las empresas, para calcular la cantidad de información que se puede transferir por una red de datos, también ayudan en el diseño de las redes de datos al implementas medidas, escalas y en el diseño del hardware que usa en las redes de computadoras.

> En el texto, se lee: "*Sistemas inteligentes aplicados*"
>
> […] "Su mayor relevancia consiste en el impacto que se espera de él para las carreras de Ingeniería, especialmente la de Computación, tanto para el rendimiento académico de los estudiante". (Bártoli, 2012)

En texto anterior se cita, los amplios recursos que tiene la Ingeniería de Sistemas, en el campo de la gestión de la información, llamada Tecnologías de las Información y las Comunicaciones (Tics), donde se estudia el uso y procesamiento de la información, dando una mayor ayuda a los procesos de gestión de la información en las empresas, también a nivel académico en investigaciones en las ciencias de la computación.

Adicionalmente la Ingeniería de Sistemas aplica las ciencias en matemáticas y física para implementar sistemas económicamente viables en beneficio de la humanidad, automatizando las tareas y procesos de datos en las empresas, así mismo salvaguardando la integridad de la información, con métodos, protocolos, reglas en seguridad informática.

> En la revista científica, e-Ciencias de la Información, se lee: "*La implementación de procesos de informatización en organizaciones como competencia en la formación de profesionales en informática*"
>
> […] "A pesar de que la implementación es una de las actividades más importantes en la formación de ingenieras e ingenieros informáticos, el análisis debe tener énfasis en el orden de las estructuras psicológicas de la personalidad". (Hernández, 2016)

La cita anterior expresa, dentro de la ciencia Ingeniería de Sistemas, el análisis de sistemas es una etapa importante en la construcción de un sistema informático, donde se recopila, interpreta, analiza y se propone una solución a futuro en la elaboración de un sistema informático, de esta etapa nace el diseño del sistema computacional que se quiere elaborar, donde se debe implementar normas de seguridad, para elaborar el código seguro con estándares de seguridad informática.

La implementación de sistemas informáticos, es la instalación, entrenamiento al usuario y la puesta en marcha de un sistema computacional. La implementación de sistemas de seguridad informática, es la instalación de herramientas tecnológicas en seguridad informática, donde se instalar programas de seguridad informática, se entrena al usuario sobre su uso y aplicación a la seguridad informática para que potencie sus conocimientos y habilidades en la defensa de ataques a la seguridad informática que puede afectar al usuario de computadora de la empresa Aguapen EP.

En el artículo científico, se lee: "*Caracterización de Herramientas de Ingeniería Inversa*"

> […] "El instrumento es validado bajo tres situaciones que demuestran su utilidad al momento de clasificar y evaluar este tipo de herramientas". (Monroy, 2012)

El texto anterior expresa la amplia gama de conocimientos y ciencias que encierra la Ingeniería de Sistemas, como es la ingeniería inversa, que trabaja en la de compilación de programas, aplicaciones y sistemas informáticos, para conocer como vulnerar sus seguridades, para hacer uso libre de las distribuciones e instalación de los sistemas informáticos con propiedad intelectual o para recuperar los programas fuentes del autor.

Para evitar que la de compilación de los sistemas no sea una tarea sencilla para los hackers, se recomienda el uso e implementación de las normas, estándares, políticas y reglas de la seguridad informática en la elaboración

del código de los sistemas informáticos y sus programas instaladores. Aumentando el nivel de seguridad con procesos de autentificación del usuario propietario de los sistemas informáticos.

2.2 Ciencias auxiliares

Las ciencias auxiliares a utilizar son la ciencia de la Seguridad Informática, las Tics y la Computación.

La ciencia de la seguridad informática, estudia los métodos de proteger la integridad de la información de los usuarios y empresas, y certifica la privacidad de los usuarios, mediante el uso de protocolos, reglas, políticas y herramientas tecnológicas, de seguridad informática, para evitar la pérdida de información o los datos, de los usuarios o empresas, asegura la privacidad de los usuarios, evitando el robo de contraseñas, identidad del usuario y información de propiedad de la empresa.

En el artículo científico, se lee: "*Seguridad Informática. Contribuciones a las Ciencias Sociales*"

> **[…] "La seguridad informática se enfoca en la protección y la privatización de sus sistemas y en esta se pueden encontrar dos tipos: La seguridad lógica que se enfoca en la protección de los contenidos y su información y la seguridad física aplicada a los equipos como tal".** (Ovalle S. O., 2012)

Como se lee en el texto anterior la seguridad informática es una ciencia muy importante dentro de la ingeniería de sistemas, que se implementa para la protección de la información, sistemas y para asegurar la privacidad de la empresa, la seguridad informática es una ciencia muy amplia y cada año crece más, debido al aumento de tipos de ataques a la seguridad informática.

Actualmente los tipos de ataques a la seguridad informática de una empresa están en aumento, y un nuevo tipo de ataque a la seguridad informática es la denegación de servicios, también llamados **DDoS**

(Distributed Denial of Service). Este tipo de ataque evita que la información de la empresa no esté disponible de forma oportuna, para sus usuarios propietarios, provocando perdida de conexión con la red, recursos y la información.

En el artículo científico, se lee: "*Modelo de Recomendación Personalizada en Cursos Virtuales basado en Computación Ubicua y Agentes Inteligentes*"

> […] "El crecimiento de la información digital sumado al auge en las telecomunicaciones de alta velocidad y la creación de sistemas ubicuos inteligentes". (Ovalle D. A., 2014)

Como se lee en la cita anterior, la ciencia de la computación ha evolucionado, ahora la información se procesa en un sinfín de equipos y dispositivos de computación, y el proceso y almacenamiento de la información también se puede realizar en la nube, mediante dispositivos inalámbricos, dispositivos móviles que trabajan con software inteligente para ayudar a las personas en su vida profesional y en sus quehaceres cotidianos dentro y fuera de su hogar.

Con el aumento de nuevas herramientas de procesos de información, como son los dispositivos móviles, también aumenta, los ataques de hackers a estos dispositivos para robar su información, robo de dinero en efectivo, y robo de su privacidad, mediante el uso mal intencionado de virus, malware y programas especializados para vulnerar la seguridad de los dispositivos móviles.

En la tesis de doctorado, se lee: "*Desarrollo de técnicas de computación evolutiva para soporte en minería de datos y texto*"

> **[…] "La obtención de información a partir de un conjunto de datos o minería de datos es una tarea compleja que involucra varias etapas, tal como sucede en la minería de texto. Esta puede ser considerada como un caso particular de minería de datos donde los datos contemplan la incorporación de texto".** (Cecchini, 2015)

En el texto anterior se expresa la necesidad del uso de la ciencia de la computación, para procesar información en pequeñas y grandes cantidades de datos, dependiendo en la ciencia que se aplica la computación, como puede ser la ciencia de la medicina, el almacenaje de la información puede ser de manera muy considerable, en su tamaño, ya que los registros que genera la ciencia de la medicina es muy amplio en todos sus campos, desde registro de pacientes, hasta el registro del genoma humano.

La ciencia de la computación comprende las bases teóricas de la información y computación con su aplicación a los sistemas computacionales, descritos como el estudio de los sistemas de procesos que dan y transforman la información, donde se mecaniza la información mediante algoritmos que trabajan procesando, almacenando, y entregando información.

En el artículo científico, se lee: "*Las Tecnologías de la Información y Comunicación en el aprendizaje*"

> **[…] "La dimensión social de las TIC se vislumbra atendiendo a la fuerza e influencia que tiene en los diferentes ámbitos y a las nuevas estructuras sociales que están emergiendo produciéndose una interacción constante y bidireccional entre la tecnología y la sociedad".** (Belloch, 2012)

En la actualidad, como expresa el texto anterior, las Tecnologías de la Información, son extensamente usadas por personas como usuarios finales y las empresas, haciendo que esta sociedad de personas se caracterice por la concentración y difusión de la información de forma masiva y con disponibilidad a tiempo completo mediante el internet.

La difusión de la información se la realiza con múltiples fines, los que pueden ser, informativos, de entretenimiento, académico, laboral, científico, empresarial, de gobiernos, etc. Para lograr esto se debe implementar una infraestructura que garantice la fluidez de la información, mediante las comunicaciones computacionales. Que permitan conectar a

los usuarios con los gobiernos, empresas, entidades públicas, instituciones escolares, etc.

2.3 La variable independiente

La variable independiente son los Problemas de seguridad Informática. Como se ha explicado anteriormente los problemas de seguridad informática no resueltos, pueden ocasionar grandes pérdidas de información, daños en los equipos de computación y pérdidas de capital en efectivo. Y toda empresa que usa sistemas computaciones, debe tener muy en cuenta los problemas de seguridad informática anteriormente descritos. Las implementaciones de las herramientas tecnológicas de seguridad informática permiten, evitar perdida de la producción de la planta de proceso de agua potable y perdida de la continuidad de los procesos administrativos de la empresa Aguapen EP.

En el artículo científico, se lee: "*Metodología para la Detección de Vulnerabilidades en Redes de Datos*"

> **[…] "Esta metodología se diferencia de otras en la medida en que se soporta cada etapa en herramientas software. Por lo que en cada fase se puntualizan las acciones que se deben realizar y cómo se deben llevar a cabo a través de las herramientas apropiadas".** (Franco D. A., 2012)

Como se lee en la cita anterior, dentro de la seguridad informática, está el estudio de la seguridad de las redes de computadoras, una red de computadoras sin la implementación de estándares de seguridad, son fácilmente vulnerables a ataques de hackers, para evitar estos problemas de seguridad en las redes de computadoras, se debe implementar normas, reglas, estándares y políticas de seguridad informática.

Para comprobar la seguridad de las redes de computadoras, se usa herramientas tecnológicas de seguridad informática, para escanear las vulnerabilidades que tiene las redes y encontrar que puertos tienen abiertos las computadoras, permitiendo el acceso a los equipos de

computación a personas sin autorización. De estas fallas de seguridad en las redes computacionales se valen los hackers para entrar sin autorización a las computadoras de los usuarios y empresas.

> En el artículo científico, se lee: "*Seguridad En Redes Industriales*"
>
> […] "Las medidas de Seguridad por una parte consisten en coacciones y restricciones, pero por otra los sistemas tienen que seguir pudiendo ser explotados y fáciles de usar para asegurar la aceptación de las medidas de seguridad por los empleados". (VARGAS, 2013)

Como expresa la cita anterior en el uso de los estándares y normas de seguridad informática se crea restricciones al uso de los dispositivos, redes y recursos informáticos de las empresas, los mismos que deben ser monitoreados constantemente para encontrar vulnerabilidades en la seguridad informática de las redes y las computadoras.

Es de suma importancia, asegurar la integridad y disponibilidad de la información de una empresa, para tener un acceso inmediato a los datos, de forma oportuna y sin restricciones, para evitar denegación del acceso a la información de la empresa, de esta manera se permite la fluidez de los procesos productivos y administrativos de las empresas.

> En el artículo científico, se lee: "*Seguridad en implementaciones de voz sobre IP*"
>
> **[…] "Algunas amenazas no son muy diferentes a las que existen actualmente en una red de datos, como por ejemplo inyecciones de SQL a nivel de aplicaciones Web, Dos (denial of service) en servicios como RDP o http y robo de sesiones o password cracking en SSH y sistemas Web".** (Oliva, 2014)

Como se lee en la cita anterior, la voz sobre ip, se ha desarrollado de una manera rápida, y las empresas han adoptado esta tecnología, para bajar sus costos en las comunicaciones, de forma efectiva. Esta nueva tecnología está basada en el protocolo de comunicaciones tcp/ip, que utiliza actualmente, el internet para la transferencia de datos, en la red mundial.

Con el surgimiento de esta nueva tecnología, también se crearon nuevas formas de atacar a los sistemas de voz sobre datos, uno de los ataques más frecuente, es el ataque DDoS, que ataca a los servidores, haciendo muchas peticiones de servicios en un segundo, para saturar sus recursos, e impedir la oportuna utilización de los servidores y sus servicios.

En tesis de grado, se lee: "*Analizando los problemas de seguridad más comunes contra las bases de datos Microsoft SQL 2008 y ORACLE 10G*"

> **[…] "El robo de información se ha vuelto la mayor amenaza para las organizaciones en estos días, los criminales han identificado donde está el dinero, dado que como todos sabemos el delito no desaparece, sino que muta, y por esto muchas son las compañías que han visto en los últimos años comprometidos sus activos intangibles, producto de haber sufrido ataques contra la confidencialidad, integridad y disponibilidad de sus bases de datos. Por lo visto, se debe tener especial cuidado sobre estas, observando los diferentes problemas de cómo pueden ser afectadas y robadas por criminales".** (Vazquez, 2012)

En el texto anterior se expresa, sobre la relevancia de salvaguardar la integridad y disponibilidad de la información de una empresa. La gran mayoría de la información esta almacenada en las bases de datos, las mismas que están alojadas en servidores de datos, al no tener políticas claras de seguridad informática, se atenta contra la seguridad de la información de las empresas.

La información es el activo intangible más valioso que tiene una empresa, porque con el pasar de los años, se acumula una gran cantidad de datos de la misma, constituyéndose esta información, en datos históricos de las empresas, esta información también es importante, para elaborar, reportes, estadísticas e informes, para los distintos entes gubernamentales y gerentes y accionistas de la empresa. Toda esta información debe ser protegida por herramientas tecnológicas de seguridad informática.

2.4 La variable dependiente

La variable dependiente son las Herramientas tecnológicas de seguridad Informática, que se utiliza actualmente para analizar, detectar, reparar y prevenir problemas de seguridad informática. Toda empresa debe hacer el uso imprescindible de las herramientas tecnológicas de seguridad informática.

Las herramientas tecnológicas de seguridad informática identifican la amenaza de manera oportuna y dan una solución al problema para minimizar los riesgos de daños a la infraestructura, evitando la perdida de información y asegurando la privacidad de los usuarios y las empresas, como Aguapen EP.

En la revista científica, se lee: "*Buenas Prácticas Para Implementación Del Comercio Electrónico En Pymes*"

> […] "La seguridad informática: es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida)". (Tarazona, 2013)

El texto anterior expresa la importancia del uso de herramientas tecnológicas de seguridad informática, para mantener las buenas prácticas de seguridad informática, para de esta manera, minimizar las vulnerabilidades y riesgos en la infraestructura, a los ataques de criminales cibernéticos. Evitando que los hackers tengan acceso a la información y privacidad de las empresas.

Para implementar un buen control, se minimiza a cero la ejecución de procesos no autorizados por los usuarios, y terceras personas, con el objetivo de evitar, daños a la infraestructura, hurto de la información y perdida de la privacidad de las empresas. Esto se logra implementando herramientas tecnológicas de seguridad informática, que controlan lo procesos no autorizados.

En el artículo científico, se lee: "*Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios*"

> **[…] "NVD (National Institute of Standards and Technology) es un repositorio estandarizado del gobierno de los Estados Unidos en el cual se encuentra almacenada información acerca de la gestión de vulnerabilidades. Estos datos permiten la automatización de la gestión de vulnerabilidades y la toma de medidas de seguridad".** (Franco D. A., 2013)

El texto anterior cita la importancia del uso de herramientas tecnológicas de seguridad informática, para encontrar vulnerabilidades y fallos de seguridad en las redes de computadoras y los equipos de computación. Recopilando información de los fallos de seguridad del National Institute of Standards and Technology de los Estados Unidos de Norte América.

Esta herramienta hace uso de la información almacenada de la gestión de vulnerabilidades encontradas en la base de datos del National Institute of Standards and Technology, para gestionar las vulnerabilidades que se encuentran en la empresa. Esta base de datos se está constantemente actualizando, con las nuevas vulnerabilidades encontradas, por diferentes fuentes de datos.

En la tesis de grado, se lee: "*Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001- sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros*"

> **[…] "En la actualidad toda empresa se basa en la información para tomar decisiones que permitan la continuidad del negocio, transformándose así en un activo importante para las organizaciones, siendo necesario protegerla ante cualquier evento que puede causar corrupción en los datos".** (Bermúdez Molina, 2015)

En la cita anterior se expresa el interés de organizaciones internacionales en salvaguardar los datos de las empresas, considerando a la información como un activo fijo muy importante, para toda empresa, y como tal, se le debe dar la protección necesaria, permitiendo con buenas prácticas de

seguridad informática, su disponibilidad inmediata, para las empresas propietarias de los datos.

Mediante el uso de estándares internacionales, buenas prácticas y herramientas tecnológicas de seguridad informática, potenciamos la integridad y disponibilidad de los datos de una empresa, la información de una empresa, se recopilo en el pasar de los años, con un costo personal-hora, al momento de tabular este costo de mano de obra, encontramos que estamos hablando de miles de dólares americanos. Si la información de una empresa se pierde, su costo de reposición es muy alto.

En la revista, Redes de Ingeniería, se lee: "*Implementación Y Actualización En La Infraestructura De Seguridad De Una Red Informática*"

> **[…] "Será implementado un nuevo cortafuego en la sucursal de zona franca, así como la creación de una VPN site to site con la sede principal. Se realizará la integración de todos los firewalls con la sede principal y la reconfiguración de rutas estáticas por mala configuración y por cambio de proveedor ISP".** (García, 2012)

En la cita anterior se expresa la necesidad del uso de herramientas tecnológicas de seguridad informática, para salvaguardar los equipos de computación, los datos y la privacidad de las empresas, al implementar estas herramientas en una empresa, se minimiza las vulnerabilidades de seguridad informática y se crea zonas seguras para trabajar con las computadoras, en cualquier empresa, que implemente las herramientas de seguridad informática.

Existen muchas herramientas tecnológicas de seguridad informática, entre las cuales podemos citar, los firewalls o también llamados muros de fuego, que trabajan denegando el acceso a peticiones de servicios a personas sin la debida autorización, para lograr con su objetivo los firewalls, manejan reglas de transporte de información de entrada y salida de un equipo de computación.

2.5 La Seguridad Informática

La Seguridad Informática se aplica a los archivos, bases de datos, metadatos, hardware y la privacidad de las personas y empresas. Para crear un ambiente libre de amenazas y vulnerabilidades en la red de datos de la empresa, cada empresa tiene sus propias políticas de seguridad informática según su conveniencia y planificación.

En el libro, se lee: "*Seguridad en Informática Aspectos Duros y Blandos*"

> […] "La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante". (Fernández J. &., 2013)

El texto anterior expresa el uso de la ciencia de Seguridad Informática en la protección de los equipos de computación, la infraestructura de computadoras, los datos, la información y la privacidad de las empresas, donde se usan los estándares y herramientas tecnológicas de computación en seguridad informática para minimizar las amenazas de seguridad informática.

La cita expresa el nivel de profundidad que comprende la salvaguarda de la información almacenada en las bases de datos, archivos de la empresa, metadatos y en especial la privacidad de la empresa, que ningún hacker acceda a la información, claves, políticas que maneja la empresa. Para evitar fuga o robo de información que se puede convertir en hurto de valores en dinero efectivo o dinero digital.

En el libro, se lee: "*La Seguridad Informática*"

> **[…] "Con el correr de los años, los seres humanos dependemos cada vez más de la tecnología para mantener nuestro estilo de vida. Ya sea para que las empresas puedan desarrollar sus negocios o para que las personas realicen sus tareas cotidianas, la tecnología siempre está ahí, simplificando las cosas".** (Portantier, 2012)

En la vida cotidiana como expresa la cita anterior, usamos muchas veces las computadoras o equipos de computación, para realizar tareas habituales para nuestro beneficio o trabajo, con el incremento de la tecnología, los equipos de computación se utilizan cada vez más en diferentes ámbitos y empresas.

Al mismo tiempo que los sistemas de computación mejoran nuestra calidad de vida, no hacemos más dependientes de los mismos, y los piratas informáticos buscan vulnerabilidades o fallos de seguridad para sacar provecho propio en el ámbito económico, robando, extorsionando, dañando y privando de privacidad a las personas y empresas.

De esta forma se debe mejorar los niveles de seguridad informática, utilizando métodos y herramientas tecnológicas en seguridad informática, para que el normal funcionamiento de los equipos de computación que usamos a diario, no se vean afectados por ataques de terceras personas

En el artículo científico, se lee: "*Informática Forense al Servicio de una Justicia Moderna*"

> […] "En los últimos años el desarrollo de las Tecnologías de la Información y las Comunicaciones (Tics) han evolucionado y permiten que sean hoy cada vez más las personas que poseen acceso a las mismas". (Semprini, 2013)

En la cita anterior observamos el incremento de problemas de seguridad informática en el mundo, a tal manera que se han creado leyes para la seguridad informática y métodos de investigación para delitos informáticos, en todos sus aspectos. Estas leyes ayudan a minimizar la incidencia de los ataques de hackers a la privacidad de las personas y empresas.

Al crear leyes que protegen al usuario y empresas de los delitos informáticos, se merma la incidencia de delitos informáticos. Asentando precedentes legales y mostrando las penas legales en la privación de la libertad de los criminales informáticos, además de la ayuda legal en cada

país, para elevar el nivel de seguridad se recomienda mucho el uso de las herramientas de seguridad informática para evitar problemas de seguridad en las computadoras y redes empresariales.

En la Revista de Ingenierías USBmed, se lee: "*Solución integral de seguridad para las pymes mediante un UTM*"

> **[…] "Este documento está enfocado a realizar un aporte teórico a la implementación de una solución de seguridad informática modular que permita integrar las funcionalidades requeridas más comunes, como son los firewall, antivirus y control de contenido, denominada como UTM (Gestor Unificado de Amenazas)".** (Flórez, 2015)

Como podemos leer en la cita anterior las ciencias computacionales siguen crecimiento y constantemente se modernizan, proveyendo al usuario y empresas mejores herramientas tecnológicas de seguridad informática, cada herramienta está enfocada de acuerdo al número de personas que tiene trabajando una empresa, así para las empresas Pymes, se recomienda el uso de firewalls, antivirus y control de contenido.

Estos controles multiplicados por el número de usuarios que tiene una empresa, da como resultado una cifra alta en el manejo de los recursos de seguridad informática. Por este motivo se debe implementar consolas de monitoreo en tiempo real, para poder observar al mismo tiempo todos los equipos de computación y sus problemas de seguridad informática.

2.6 Amenazas a la seguridad Informática

Las amenazas a la seguridad informática nacen de los errores de seguridad en las redes de computadoras, líneas de codificación de los programas, y por el no uso de buenas prácticas de seguridad informática en los equipos de computación y servidores de datos. Que no han sido atendidos en seguridad informática de forma oportuna con normas de seguridad para cuidar la integridad de los datos.

En la revista, scielo, se lee: "*Gestión automatizada, e integrada de controles de seguridad informática*"

> **[…] "La seguridad informática, o seguridad de la información, es la preservación de la confidencialidad, integridad y disponibilidad de la información. Esto se logra mediante la implantación de un grupo de controles que incluyen políticas, procedimientos, estructuras organizativas y sistemas de hardware y software".** (Montesino Perurena, 2013)

En la cita anterior se expresa la necesidad de hacer un continuo monitoreo a las actividades y usos de las computadoras de las empresas, las redes de datos y los servidores de datos, para encontrar de forma proactiva fallos en la seguridad informática, para esto se deben implementar mecanismos de verificación, monitoreo y testeo a los problemas de seguridad informática de una empresa.

Adicionalmente es muy recomendable implementar las normas ISO/IEC 27001, para el control de la calidad, en la implementación de las normas, políticas y reglas de seguridad informática, en los equipos de computación de toda empresa, para asegurar la disponibilidad de su información.

En el artículo científico, se lee: "*Análisis de Riesgos en Seguridad de la Información*"

> […] "Con el crecimiento y auge de las Nuevas Tecnologías de la Información y la Comunicación (TIC), los avances en los servicios y modelos de comunicaciones e información, el uso continuo y generalizado a nivel global de la Internet". (Abril, 2014)

Como expresa la cita anterior, con el crecimiento de las tecnologías de la información y comunicaciones, la cual es una rama de la ingeniería en Sistemas, también crecen las amenazas de seguridad informática, con cada nueva tecnología que aparece, los hackers, buscan vulnerabilidades, en los sistemas y equipos de computación, que puedan explotar, mediante, escaneo de puertos abiertos, escaneo de la red, para encontrar una puerta abierta, por la que pueda atacar y usurpar la privacidad del usuario.

La mejor forma de arreglar un problema es la prevención, por este motivo se debe estar un paso más adelante de los hackers informáticos, buscando vulnerabilidades en los equipos de computación de la empresa, con programas tecnológicos de seguridad informática, una vez hallada la vulnerabilidad proceder con la respectiva reparación, en el software, mediante actualizaciones de seguridad.

En el artículo científico, se lee: "*Seguridad y Amenazas en la Información*"

> […] "Los datos que maneja el sistema serán los más importantes ya que son el resultado del trabajo realizado. si existe daño del hardware, software o de los elementos fungibles, estos pueden adquirirse nuevamente desde su medio original". (Cuevas Martínez, 2012)

La cita anterior expresa la importancia de minimizar las amenazas a la seguridad informática de una empresa, empleando el uso de herramientas tecnológicas de seguridad informática, para evitar, que personas mal intencionadas, hurten la información de la empresa o la dañen, para esto se debe hacer un monitoreo continuo, a los equipos de computación, a los sistemas computacionales y servidores de datos de la empresa.

Los datos de la empresa, son los activos fijos intangibles, más valiosos que tiene la misma, por su alto costo en su creación, y almacenar información crítica de los procesos productivos y administrativos de la empresa, del año en curso y datos históricos, los cuales, si se llegaran a perder, tendría un costo muy elevado, para su recuperación, y cuando se recupere la información perdida, no quedaría igual como estaba en su estado original.

2.7 Tipos de amenazas a la Seguridad Informática

Las amenazas de seguridad informática surgen de la programación y los medios de almacenamiento, transmisión o proceso de los datos, además hay otros problemas de seguridad externos a la empresa, que se deben tener en consideración, para asegurar un alto nivel de seguridad

informática debemos usar la prevención a cualquier tipo de problema en seguridad y siniestros que pueden afectar a una empresa. Las amenazas más comunes son:

Los usuarios: son el mayor problema de seguridad informática. Al tener permisos sobredimensionados, causan daños en la información de forma voluntaria o involuntaria

Programas maliciosos: programas diseñados para hacer un uso ilícito de los datos de una empresa. Para provocar daños se instalan en una computadora, abriendo una puerta para permitir el ingreso a personas no autorizadas a la información, este tipo de programas puede ser un virus, malware, un gusano informático, un troyano, una bomba lógica, un programa espía.

Los errores de programación: este tipo de amenaza informática explota errores de seguridad en la codificación de los programas, y son usados por los crackers, para remediar estos errores se crearon las actualizaciones y parches a los sistemas operativos o programas utilitarios.

Los intrusos: son personas no autorizadas al acceso de la información de una empresa, y se los considera como hackers.

Siniestros externos: otra amenaza a la seguridad informática son los siniestros de tipo externo, que ocasionan graves daños a la información, los mismos que pueden ser irreversibles, dentro de los cuales son: incendios, catástrofes naturales, manipulación malintencionada de la información, perdida de la información a propósito

Personal técnico de la empresa: son los técnicos de sistemas, administradores de bases de datos, desarrolladores, etc. Por motivos de problemas laborales, altercados internos, destituciones, enriquecimiento ilícito, espionaje. Causan daño en la información de la empresa.

Los fallos electrónicos: estos problemas a la seguridad informática son muy habituales, por ende, se debe tener implementada respaldos de energía eléctrica, también contar con una adecuada instalación eléctrica para computadoras.

El malware, es un tipo de virus malicioso, que se distribuye por internet, para infectar de forma anónima las computadoras de los usuarios, generalmente se esconde, en programas infectados, páginas web maliciosas y emails.

Virus, es un programa malicioso, que tiene la capacidad de reproducirse a sí mismo, con el objetivo de propagarse en otras computadoras, por medio de redes de datos e internet, su fin, es de causar daño o robar la información de los usurarios

> En el libro, se lee: "*Ethical Hacking 2.0*"
>
> **[…] "El espionaje corporativo existe como tal, prácticamente desde la revolución industrial, cuando los secretos productivos de las fabricas comenzaban a ser la clave de los negocios. Con el correr del tiempo, estos secretos fueron tomando la forma de fórmulas químicas, procesos productivos, materiales especiales, proyectos de investigación y desarrollo, y campañas publicitarias".** (Jara, 2012)

Como cita el texto anterior, algunos problemas de la seguridad informática, se iniciaron con la competencia entre empresas, por querer hurtar información valiosa de las empresas, por personas con falta de ética. Estas empresas maliciosas, emplearon estas malas prácticas, para competir, de una forma desleal, en el mercado de consumo. Y de esta forma robar el activo intangible, más valioso, que es la información de una empresa.

Estas prácticas de sustracción de información, permitieron que se empleen nuevos métodos, de ciber espionaje, que se desarrollaron, según las necesidades, de las personas, que querían sustraer información privilegiada de las empresas. Para evitar la fuga de información, se debe

implementar herramientas tecnológicas de seguridad informática, que permitan hacer un monitoreo constante, de las actividades en los equipos de computación, y utilizado restricciones a los accesos a los equipos de computación y su información.

En el artículo científico, se lee: "*Estándares para minimizar ataques de seguridad en los Servicios Web*"

> **[…] "Un atacante puede interceptar un mensaje, modificar el encabezado y el cuerpo (rutas y/o sentencias XML) y enviarlo repetidamente para sobrecargar el servicio del intermediario o del destino final, con lo cual logra que el servidor o el intermediario no pueda atender a un consumidor legítimo".** (Martínez, 2012)

Como expresa la cita anterior, una nueva forma de problema de seguridad, en los servidores de datos y web, es la denegación de acceso, a la información, para un usuario legítimo, al no permitir la conexión al servidor, al usuario se le priva, de su información, este problema, es uno, de los más graves, porque a la empresa se le priva de su información.

Este problema se provoca, cuando se hace muchas peticiones de conexión al servidor, saturando su funcionamiento, al saturar la capacidad de proceso, el servidor de datos o web, no permite más accesos a su información. Impidiendo que el usuario legitimo acceda a sus datos. Para arreglar este ataque de denegación de acceso, se debe implementar el uso de herramientas tecnológicas de seguridad informática.

En el texto, se lee: "*Inseguridad Cibernética, en América Latina*"

> […] "Un análisis sencillo de las administraciones de los países de América Latina permite constatar que instituciones especializadas en la lucha contra la ciberdelincuencia generalmente existen". (MARTIN, 2015)

Como expresa la cita anterior, existen organizaciones internacionales, para contrarrestar la ciberdelincuencia, que dan apoyo a las empresas para que se protejan de los ataques por parte de delincuentes cibernéticos, pero esta ayuda no es suficiente, cuando la empresa no hace conciencia de sus problemas de seguridad informática. Y hace caso

omiso a las alertas y programas de seguridad de las instituciones internacionales expertas en seguridad informática.

Un problema común de seguridad informática, es la falta de interés de las empresas de proteger sus equipos de cómputo o datos, no asignado un presupuesto para la seguridad informática, este desinterés por parte de las empresas provoca la mayoría de los ataques a la seguridad informática, porque el atacante encuentra, en estas empresas un paraíso para hacer sus fechorías, por falta de la implementación de herramientas tecnológicas de seguridad informática.

En el texto, se lee: "*Tipos De Ataques E Intrusos En Las Redes Informáticas*"

> […] "Los programas de software espía o los dispositivos hardware especializados que permitan registrar todas las pulsaciones en el teclado de un ordenador ("keyloggers"). De hecho, es posible localizar soluciones disponibles en el mercado como KeyGhost (www.keyghost.com) o KeyLogger (www.keylogger.com)". (Vieites, 2013)

Como cita el texto anterior, los piratas cibernéticos se valen de programas maliciosos, para robar información de los usuarios, como sus claves, haciendo uso de software espía, que captura las claves digitadas por el usuario y la envía, por medio de internet al hacker propietario de este programa malicioso.

Para evitar la suplantación de identidad, por medio del robo de claves a los usuarios, se debe implementar en primer lugar, de restricción de acceso a los equipos de computación, a las personas no autorizadas, por medio de herramientas tecnológicas de seguridad informática, donde se implementan reglas de acceso y uso de los equipos de computación.

2.8 Integridad de la Información

Dentro de la ingeniería en Sistemas Computacionales, encontramos la seguridad informática o también llamada, Seguridad de las Tecnologías

de la Información. Es la ciencia, de la informática que estudia la defensa de los equipos de computación y la información, de los hackers, aplicando, estándares, protocolos, métodos, reglas, herramientas, y leyes, con el objetivo, de minimizar las amenazas a la seguridad informática.

En el artículo científico, se lee: "*Integridad de Datos en Sistemas de Gestión de Aprendizaje*"

> **[…] "Partiendo de la premisa de que todo sistema con múltiples puntos de acceso, requiere de alta confiabilidad y seguridad, es claro que un punto fundamental es garantizar la integridad de los datos compartidos como uno de los temas de importancia relacionados con la seguridad".** (Fritz, 2015)

El texto anterior expresa la necesidad de subir los niveles de seguridad en todo sistema de información, en especial los sistemas de información con ambiente web, con el objetivo de entregar los datos al usuario propietario, sea información legitima y precisa, los hackers están interesados en robar o distorsionar estos datos, por lo que es necesario implementar medidas de seguridad para garantizar la integridad de la información.

Es importante implementar herramientas de seguridad informática, en todo sistema de información de acceso público o privado, para asegurar la confiabilidad de los datos y su disponibilidad inmediata, para sus legítimos dueños o empresas, esto se puede lograr estableciendo normas, reglas, políticas de seguridad informática y restringiendo el acceso al personal no autorizado, a la información de la empresa.

En el artículo científico, se lee: "*Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes*"

> **[…] "En la actualidad, las empresas de cualquier tipo o sector de actividad se enfrentan cada vez más con riesgos e inseguridades procedentes de una amplia variedad de contingencias, las cuales pueden dañar considerablemente tanto los sistemas de información como la información procesada y almacenada".** (Fernández L. G., 2012)

La cita anterior expresa, la relevancia de categorizar a la información, como el activo fijo intangible más importante de la empresa, por ende, se debe prestar un especial cuidado, a la integridad de la información, asegurando su integridad y resguardo con todos los métodos de seguridad informática que le sean posibles a la empresa.

La información de tener un alto grado de confiabilidad, integridad y disponibilidad en toda empresa, para esto la empresa debe asignar un presupuesto especial a la seguridad informática, para implementar herramientas tecnológicas de seguridad informática, las cuales necesitan de una inversión de dinero, además la empresa debe contar con personal capacitado para la implementación de las herramientas de seguridad.

En el artículo científico, se lee: "*Establecimiento y diseño de los entregables para la implementación de la norma técnica de seguridad de la información ISO/IEC 27002:2013*"

> **[…] "La seguridad informática es un proceso que busca establecer mecanismos para conservar en primera instancia la confidencialidad, integridad y disponibilidad de la información, considerando a ésta como el activo con mayor importancia que poseen las organizaciones".** (Sisalima, 2015)

El texto anterior cita, los nuevos métodos que usan los delincuentes cibernéticos, para hurtar la información, están en aumento, y cada vez son más sofisticados, por este motivo las empresas buscan los mejores métodos y herramientas de seguridad informática para defenderse de los ataques a las vulnerabilidades en seguridad informática.

Estos nuevos métodos para sustraer información de los usuarios o empresas, se especializan en explotar las vulnerabilidades de seguridad de los equipos de cómputo y software. Y cada día los ataques a las vulnerabilidades en seguridad informática, son más sofisticados y meticulosamente planeados. Para salvaguardar la integridad de la información, se debe hacer un constante monitoreo, a las actividades de los equipos de computación y a sus usuarios.

En la tesis de grado, se lee: "*Cumplimiento De Normas De Seguridad, De Las Bases De Datos*"

> **[…] "El propósito de este estudio es reducir el riesgo asociado al uso de bases de datos que no cumplen con las normas de seguridad, además analizar efecto en el riesgo que causa la seguridad de la información de las empresas".** (ESTRADA ROJAS, 2016)

El texto anterior cita, los datos de la empresa también, están almacenados en las bases de datos, los datos almacenados en una base de datos, son imposibles de recuperar, cuando la base de datos, se daña, por cualquier motivo, por esto, se debe implementar mecanismos y políticas de recuperación de la información en caso que ocurra un siniestro que afecte a la base de datos.

Para salvaguardar los datos almacenados en las bases de datos, de posibles daños, perdida, hurto, cataclismos, incendios, que pueden sufrir de los datos de la empresa, se debe implementar políticas de seguridad, donde se establezca un plan de respaldos a las bases de datos y un plan de recuperación de la información, en caso de algún siniestro.

2.9 Normas Cobit 5

Las normas Cobit 5, son aceptadas internacionalmente, para las buenas practicas, en el control de la información, TI, y los riesgos que conllevan. Cobit se utiliza para implementar el gobierno de TI y mejorar los controles de TI.

En el libro, Cobit, se lee: "*Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*"

> **[…] "Las empresas existen para crear valor para sus accionistas. En consecuencia, cualquier empresa, comercial o no, tendrá la creación de valor como un objetivo de Gobierno. Creación de valor significa conseguir beneficios a un coste óptimo de los recursos mientras se optimiza el riesgo".** (ISACA, 2012)

Las normas Cobit, son reconocidas internacionalmente, para el uso de buenas prácticas en el manejo de la información, aquí se hace referencia a las normas, reglas, políticas y estándares de seguridad informática, para cuidar la disponibilidad de la información, en toda empresa.

Como expresa el texto anterior, toda empresa, se crea para generar beneficios, a sus accionistas, y sus actividades comerciales conllevan un riesgo comercial, para ser más competentes las empresas, utilizan las tecnologías de la información TICs, donde surgen nuevos riesgos, entorno a la seguridad informática, por ende, toda empresa, debe hacer uso, de las normas para las buenas prácticas, en seguridad informática, para salvaguardar la integridad y accesibilidad de la información.

2.10 Reseña de la Empresa Pública Municipal Aguapen EP

La Empresa Pública AGUAPEN-EP, en sus inicios, fue empresa privada, y constituida legalmente el 14 de diciembre de 1999, con el objetivo de servir con en alcantarillado sanitario, alcantarillado pluvial, tratamiento de aguas servidas y de agua potable en la provincia de Santa Elena.

En abril de 2011, la empresa AGUAPEN EP, hizo cambio de personería jurídica. Con el apoyo de los GADs de los cantones de La Libertad, Santa Elena y Salinas. Se constituyó en la Empresa Pública Municipal Mancomunada Aguapen-EP, regida por los tres Gobiernos Autónomos Municipales de La Libertad, Salinas, y Santa Elena, cuyos Alcaldes conforman el Directorio de la empresa Aguapen EP.

La nueva personería jurídica la empresa Aguapen-EP, se publicó, con el registro oficial No 810, el 16 de octubre del 2012. El actual Gerente General de la empresa es el Ing. Gino Arturo Farfán Pazos.

CAPITULO III

3. La Investigación

Esta investigación se basa en el trabajo de campo y la observación del parque de computadoras de la empresa Aguapen EP, para encontrar problemas de seguridad informática, en los equipos de computación de la empresa antes mencionada.

La epistemología, es la teoría del conocimiento, que trabaja con las circunstancias históricas, psicológicas y sociológicas, que llevan a la obtención del conocimiento, y se enfoca en la relación sujeto – objeto, para este objetivo, usa criterios que justifican o invalidan, el conocimiento.

3.1 Epistemología de la Investigación

El método que vamos a usar, para conocer el Sujeto – Objeto en la investigación, es la Epistemología Empirista, porque esta escuela de pensamiento se basa en conocimiento científico, y afirma, que toda la verdad a ser investigada, está en el objeto.

3.2 Diseño de la Investigación

El diseño de la investigación, es no experimental – transaccional, porque la investigación está basada en el trabajo de campo y se enfoca en la observación del objeto. Para recolectar datos de la unidad de observación y publico muestral.

3.3 Tipo de Investigación

El tipo de investigación a utilizar es, la investigación descriptiva, porque vamos analizar las variables, con sus dimensiones y sus indicadores. Para describir sus datos, tomando en cuenta el impacto en la unidad de observación.

3.4 Métodos de investigación

El método de investigación que se va a usar es, el método Hipotético – Deductivo, porque, se plantea una hipótesis y se elabora una encuesta. La encuesta se plantea, para observar los resultados obtenidos, y estos resultados ayudaran en la comprobación de la hipótesis. Y la exploración de documentos en internet, de empresas especializadas en seguridad informática

3.5 Hipótesis

Las herramientas tecnológicas de seguridad informática, solucionan los problemas de vulnerabilidad de seguridad informática, en el parque de computadoras de la empresa Aguapen EP.

3.5.1 Detección de las variables

La variable A es: problemas de Seguridad informática en el parque de Computadoras de la empresa Aguapen EP

La variable B es: herramientas tecnológicas para solucionar problemas de la seguridad informática de la empresa Aguapen EP.

3.5.2 Definición conceptual de las variables

La variable A (problemas de Seguridad informática en el parque de Computadoras de la empresa Aguapen EP), se define como, los problemas de seguridad informática, encontrados en el parque de computadoras de la empresa Aguapen EP, que afectan a la infraestructura computacional, los datos y la privacidad de la empresa Aguapen EP, y son ocasionados por personas que no tienen autorización del uso y acceso a los equipos de computación de la empresa.

En la tesis de grado, se lee: "*Plan de seguridad de la información, basado en el estándar iso 13335*"

> […] "De acuerdo con el Instituto de Seguridad Informática (CSI) de San Francisco, aproximadamente entre 60 y 80 por ciento de los incidentes de red son causados dentro de la misma empresa". (ALVARADO, 2013)

Como expresa el texto anterior, los problemas de seguridad informática, se incrementan, cuando los equipos de computación están conectados, a una red de computadoras, con más incidencia, si las computadoras están conectadas al internet.

El hecho que un equipo de computación no esté conectado a una red, no garantiza, la seguridad computacional, de una computadora, según los estudios realizados por el Instituto de seguridad Informática (CSI), casi un 80 por ciento de los casos, de vulneración a la seguridad informática, fueron causados por personal de la misma empresa.

La variable B (Herramientas tecnológica para solucionar problemas de la seguridad informática de la empresa Aguapen EP), se define como, las herramientas tecnológicas de seguridad informática identifican la amenaza de manera oportuna y dan una solución al problema para minimizar los riesgos de daños a la infraestructura, evitar perdida de información y asegurar la privacidad de la empresa Aguapen EP

En el artículo científico, se lee: "*Vulnerabilidad de Ambientes Virtuales]*"

> […] "Así como también, se propone algunos criterios a evaluar en cuanto a seguridad de información, en AVA y posteriormente se realiza el proceso de análisis de seguridad, por medio de las herramientas SQLMap, RIPS, W3AF y Nessus." (López, 2014)

Como cita el texto anterior, son numerosos los casos de ataques a la seguridad informática, que sufren las computadoras conectadas al internet, el motivo de la gran cantidad de ataques a las computadoras conectadas al internet, es porque el internet está conectado a una red mundial de computadoras, en todo el mundo.

Para analizar y corregir las vulnerabilidades de seguridad informática de las computadoras, se debe hacer uso de las herramientas tecnológicas de seguridad informática, como son: SQLMap, RIPS, W3AF y Nessus, entre otras, de esta forma incrementaremos la seguridad informática, encontrando y corrigiendo vulnerabilidades de seguridad en las computadoras de la empresa

3.5.3 Definición real de las variables

La empresa Aguapen EP, cuenta en la actualidad con un parque de computadoras, de ochenta equipos de computación personal, en los cuales se ha encontrado problemas de seguridad informática, como, la perdida de los datos, por mal uso o desconocimiento de los usuarios. Además, se ha encontrado múltiples veces, virus de tipo troyano y malware, que han provocado perdida de los datos de la empresa, daños en los equipos de computación, y perdida de la producción administrativa, por el tiempo que se empleó para reparar los equipos de computación.

3.5.4 Definición operacional de las variables

Tabla 1 “Definición operacional de la variable Independiente”

Variable Independiente: Problemas de Seguridad informática en el parque de Computadoras de la empresa Aguapen EP					
Conceptualización	**Dimensiones**	**Indicadores**	**Ítems**	**Fuentes**	**Instrumentos/ Técnica**
La seguridad informática, salvaguarda los datos y la privacidad, de la empresa para evitar y corregir problemas relacionados al uso no autorizado de computadoras y datos	Virus	• Troyanos • Malware • Keylogger	Que tipos de virus se encuentra en el parque de computadoras de la empresa Aguapen EP?	Parque de computadoras de la empresa Aguapen EP	Entrevista
	Acceso no autorizado a las computadoras	• Daño de información • Perdida de información • Perdida de la integridad de la información	Que tipos de accesos no autorizados se encuentra en el parque de computadoras de la empresa Aguapen EP?	Parque de computadoras de la empresa Aguapen EP	Entrevista

Elaborado por: El autor

Tabla 2 “Definición operacional de la variable dependiente”

Variable dependiente: Herramientas tecnológica para solucionar problemas de la seguridad informática de la empresa Aguapen EP					
Conceptualización	**Dimensiones**	**Indicadores**	**Ítems**	**Fuentes**	**Instrumentos/ Técnica**
Las herramientas tecnológicas de seguridad informática identifican la amenaza de manera oportuna y dan una solución al problema para minimizar los riesgos de daños a la infraestructura, evitar perdida de información y asegurar la privacidad de la empresa Aguapen EP	Herramientas de seguridad informática	• Seguridad para estaciones de trabajo • Administración y seguridad móvil multicapa • Anti malware • Consola de administración centralizada para todas las funciones	¿Qué tipo de seguridad informática ofrece las herramientas de seguridad informática?	Herramientas de seguridad informática	Encuesta

Elaborado por: El autor

3.6 Técnicas de investigación

Las técnicas de investigación se enfocan a la variable, problemas de seguridad informática, para este objetivo se elabora una encuesta a los usuarios de las computadoras de la empresa Aguapen EP, y se investiga, en las empresas especializadas, en hacer test y calificar a las herramientas tecnológicas de seguridad informática. Para saber cuál es la mejor solución para los problemas de seguridad informática.

La encuesta, se forma una pregunta de una línea, al final se pide a la persona encuestada que responda si / no

El análisis de los documentos, utiliza el sentido de la vista para analizar lo que necesitamos seleccionar, describir y explicar, en documentos escritos o en formato digital.

3.7 Población y muestra

Para efectuar el respectivo análisis cuantitativo de esta investigación, una vez definidos el tipo de investigación y sus técnicas para recolectar los datos, la población está ubicada en la empresa Aguapen EP de la ciudad de Salinas, provincia de Santa Elena, haciendo un conteo in sitio, se contabilizo 80 equipos de computación, donde se aplicará el uso de una muestra con un porcentaje de fiabilidad del 90%, con este objetivo se planifica usar el método de muestreo probabilístico. Para calcular el valor de muestra se aplica la siguiente formula:

N = Tamaño de la muestra (Población de 80 computadoras)
Z = 1.65 para un nivel de confianza del 90%
p = Probabilidad de ocurrencia (éxito 50%)
q = Probabilidad de no ocurrencia (no éxito 50%)
e = error de muestreo (9%)

$$\mathbf{n=} \frac{z^2 . N . p . q}{e^2 . (N-1) + z^2 . p . q}$$

$$n = \frac{(1.65)^2 . 80 . 0.5 . 0.5}{((0.09)^2 . (80-1)) + ((1.65)^2 . 0.5 . 0.5)}$$

n= 41

El tamaño de la muestra es 41 personas, este es la cantidad de personas a las que se debe aplicar la encuesta, para tener una muestra que represente a la población,

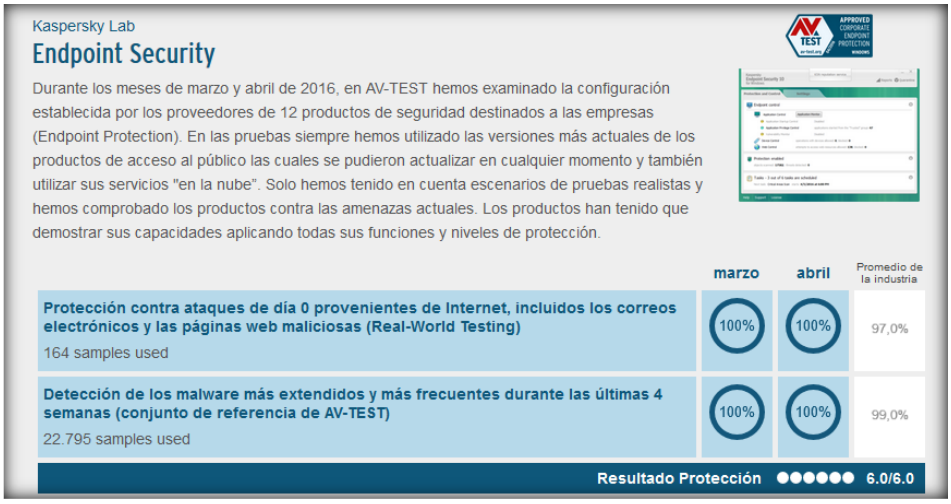
3.8 Análisis de evaluación del producto de seguridad informática

Para el análisis, se procedió a investigar en internet, el ranking de "Evaluaciones y calificaciones a las herramientas empresariales de seguridad informática", por el Instituto de AV-Test y la empresa especializada, Virus Bulletin's testing and certification services, donde se encontró los siguientes resultados:

3.8.1 El Institutito AV-TEST

El Instituto AV-Test es un servidor independiente y líder mundial de servicios en el campo de la seguridad informática y de la investigación antivirus. Da los siguientes resultados:

Figura 1"Calificación para Kaspersky Lab Endpoint Security"



Elaborado por: El autor

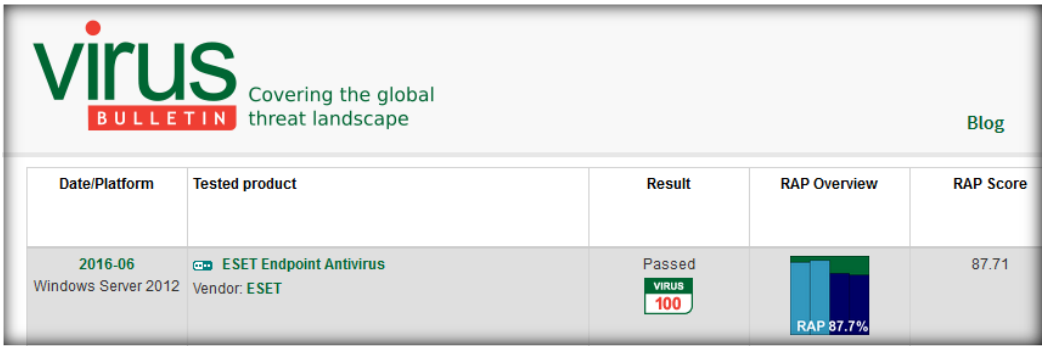
Fuente: (www.av-test.org, 2016)

El Instituto AV-Test especializado, en test y certificaciones de antivirus, para la herramienta empresarial de seguridad informática, Kaspersky Lab Endpoint Security, da una calificación de 6.0/6.0, equivalente a 100 puntos sobre 100, la cual es la máxima calificación a una herramienta de seguridad informática tipo empresarial, que se encuentra, en el mercado actualmente.

3.8.2 Virus Bulletin's testing and certification services

Según la empresa especializada de test y certificación de antivirus, “Virus Bulletin's testing and certification services”, da los siguientes resultados para el antivirus Eset para empresas:

Figura 2“Calificación para Eset Endpoint”



Elaborado por: El autor

Fuente: (https://www.virusbulletin.com, 2016)

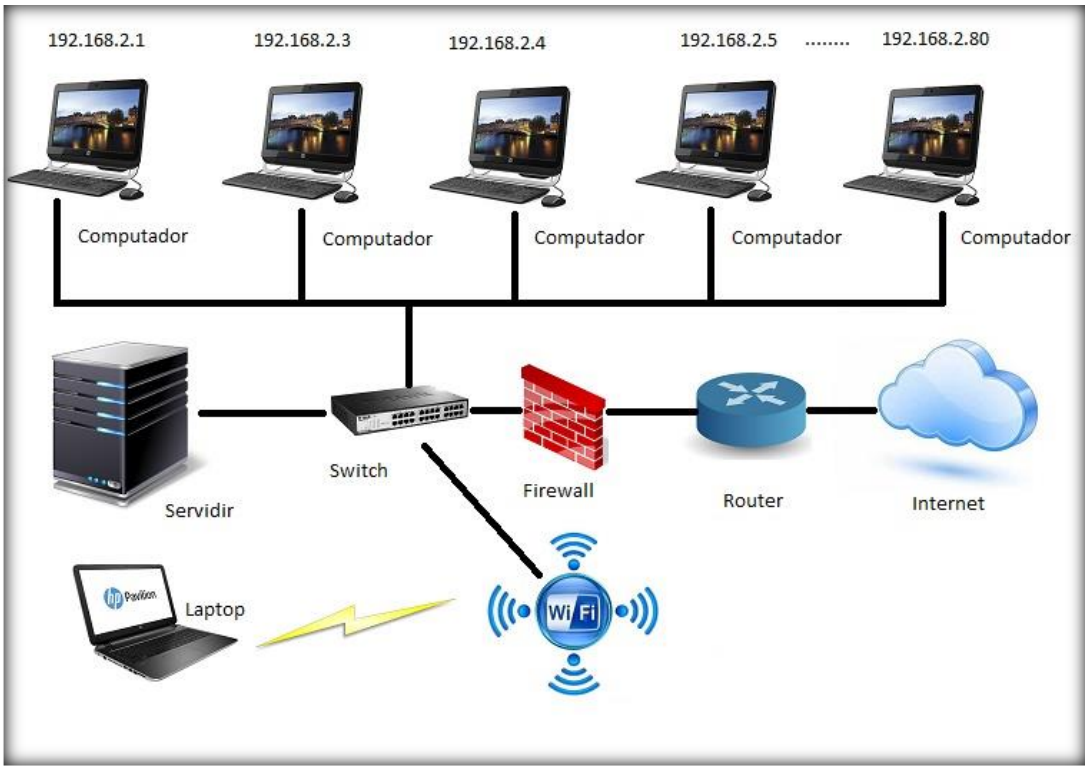
La empresa especializada en test y certificaciones de antivirus, “Virus Bulletin's testing and certification services”, para la herramienta empresarial de seguridad informática, Eset Endpoint Antivirus, da una calificación de 87,71 sobre cien.

3.8.3 Diagrama de red de la empresa Aguapen EP

El diagrama de la red, de la empresa Aguapen EP, trabaja en el segmento de red 192.168.2.1 hasta la ip, 192.168.2.80. Donde se puede observar que no tiene un servidor de dominio para autentificar los accesos de las computadoras a la red.

Para conectar las computadoras a la red, usa switchs en cascada, y para hacer la conexión a internet, emplea un firewall y un router, como se puede ver en la figura 3.

Figura 3 Diagrama de red de la empresa Aguapen EP



Elaborado por: El autor

CAPITULO IV

4. Análisis de los Resultados

Después de ejecutar las respectivas encuestas (mediante una muestra de la población), a los usuarios de las computadoras de la empresa Aguapen EP, para la recopilación de la información, se procede a procesar la información, creando tablas, gráficos, para su posterior análisis. Los datos que encontremos en el análisis de los resultados, orientarán a elaborar las conclusiones de la presente investigación

Después de realizar la respectiva encuesta, a la muestra de la población, del parque de computadoras, de la empresa Aguapen EP, se procede a tabular la información, por medio de tablas y posteriormente se elabora su respectivo gráfico, a cada pregunta formulada en la encuesta.

Los resultados de la encuesta, se tabularon en Excel, y se muestran a continuación, donde se muestran las vulnerabilidades de seguridad informática, que se encontraron en las computadoras.

Adicionalmente, a continuación, se muestra los resultados de la exploración, del análisis de la evaluación de los productos de seguridad informática.

4.0.1 Análisis de los Resultados de la encuesta

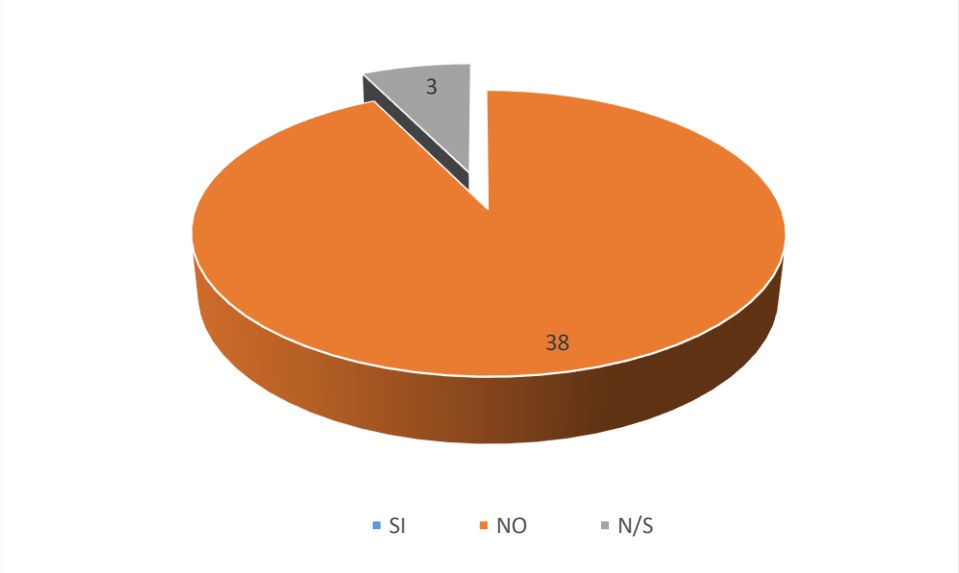
Tabla 3 " La computadora tiene instalado un antivirus empresarial "

RESPUESTA	CANTIDAD	PORCENTAJE
SI	3	7,32%
NO	30	73,17%
N/S	8	19,51%
Total:	41	100%

Elaborado por: El autor

Fuente: encuesta in situ

Gráfico 1 “La computadora tiene instalado un antivirus empresarial”



Elaborado por: El autor

Fuente: encuesta in situ

La encuesta muestra, en la pregunta uno, “¿Su computadora tiene instalado un antivirus de tipo empresarial?”, que le 73,17 % de las personas encuestadas, no tiene un antivirus de tipo empresarial, instalado en su computadora, lo que permite observar, la necesidad de adquirir, una herramienta de seguridad informática para la empresa Aguapen EP

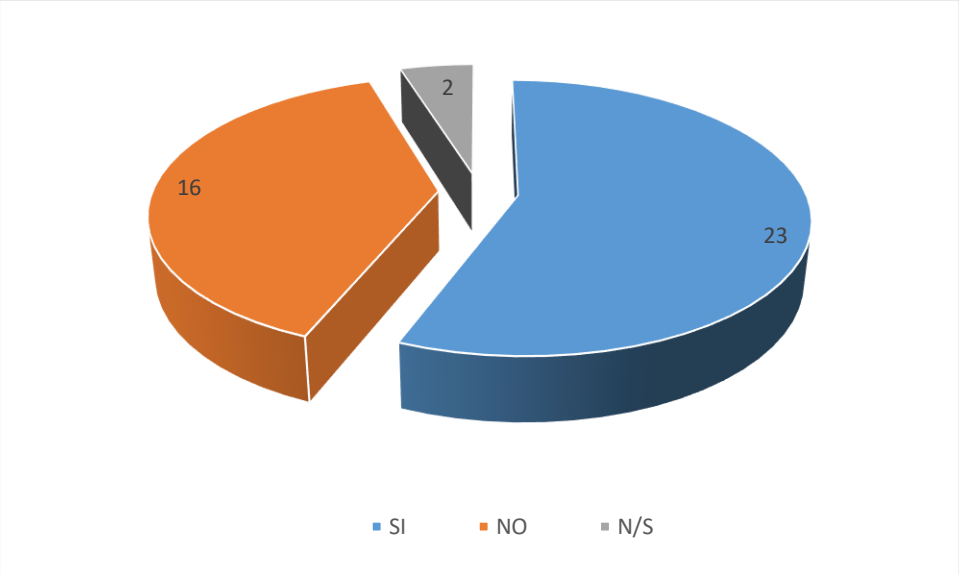
Tabla 4 "La computadora ha tenido problemas de virus"

RESPUESTA	CANTIDAD	PORCENTAJE
SI	23	56,10%
NO	16	39,02%
N/S	2	4,88%
Total:	41	100%

Elaborado por: El autor

Fuente: encuesta in situ

Gráfico 2 “La computadora ha tenido problemas de virus”



Elaborado por: El autor

Fuente: encuesta in situ

La encuesta muestra, en la pregunta dos, “¿Su computadora ha tenido problemas de virus?”, que el 56,10% de las personas encuestadas, ha tenido problemas de virus, en sus computadoras, por lo que se observa, que tienen problemas de vulnerabilidades de seguridad informática.

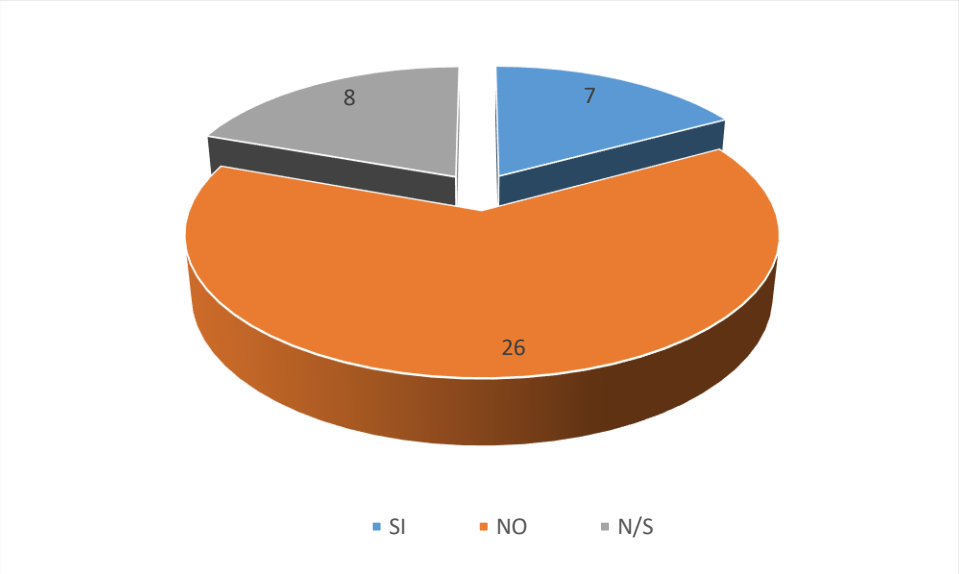
Tabla 5 "Computadora ha tenido ataques de captura de teclado"

RESPUESTA	CANTIDAD	PORCENTAJE
SI	7	17,07%
NO	26	63,41%
N/S	8	19,51%
Total:	41	100%

Elaborado por: El autor

Fuente: encuesta in situ

Gráfico 3 “Computadora ha tenido ataques de captura de teclado”



Elaborado por: El autor

Fuente: encuesta in situ

La encuesta muestra, en la pregunta tres, “¿Su equipo de computación ha tenido ataques de captura de teclado?”, que el 17,07 % de las personas encuestadas, han tenido ataques de personas no autorizadas, al uso del equipo de computación.

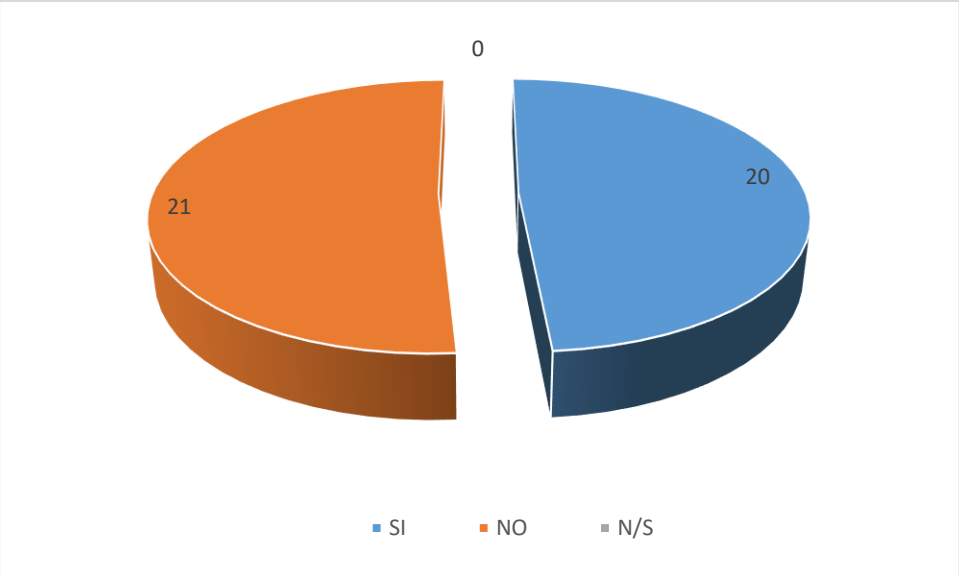
Tabla 6 "El usuario encontró archivos dañados en su computador"

RESPUESTA	CANTIDAD	PORCENTAJE
SI	20	48,78%
NO	21	51,22%
N/S	0	0,00%
Total:	41	100%

Elaborado por: El autor

Fuente: encuesta in situ

Gráfico 4 “El usuario encontró archivos dañados en su computador”



Elaborado por: El autor

Fuente: encuesta in situ

La encuesta muestra, en la pregunta cuatro, “¿Usted ha encontrado archivos dañados en su computador?”, se observa que el 48,78 % de las personas encuestadas, encontraron sus archivos dañados, lo cual es preocupante porque existe un alto riesgo de ataques a la seguridad de la información.

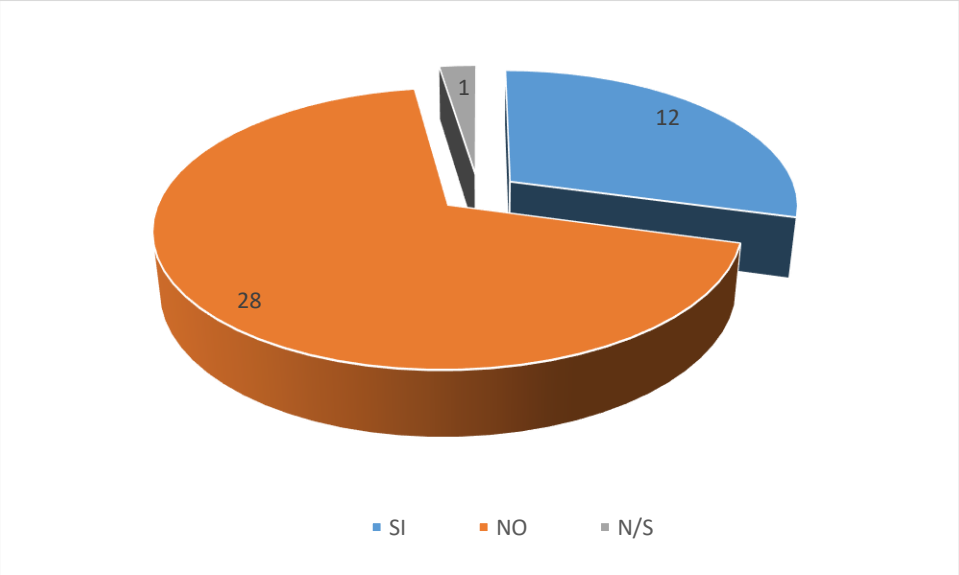
Tabla 7 "Pérdida de información"

RESPUESTA	CANTIDAD	PORCENTAJE
SI	12	29,27%
NO	28	68,29%
N/S	1	2,44%
Total:	41	100%

Elaborado por: El autor

Fuente: encuesta in situ

Gráfico 5 “Pérdida de información”



Elaborado por: El autor

Fuente: encuesta in situ

La encuesta muestra, en la pregunta cinco, “¿Usted ha tenido perdida de información?”, que el 29,27 % de las personas encuestadas, tuvieron problemas de pérdida de información, lo que evidencia problemas de vulnerabilidad a la seguridad informática.

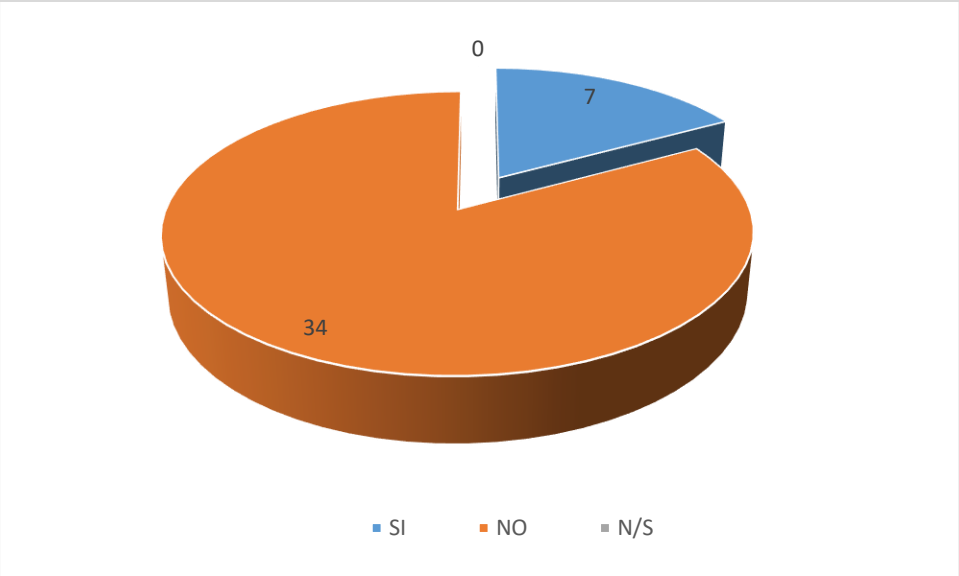
Tabla 8 "Archivos con la información cambiada"

RESPUESTA	CANTIDAD	PORCENTAJE
SI	7	17,07%
NO	34	82,93%
N/S	0	0,00%
Total:	41	100%

Elaborado por: El autor

Fuente: encuesta in situ

Gráfico 6 “Archivos con la información cambiada”



Elaborado por: El autor

Fuente: encuesta in situ

La encuesta muestra, en la pregunta seis, “¿Usted ha encontrado archivos con la información cambiada?”, se observa que 17,07 % de las personas encuestadas, han tenido ataques, a la integridad de la información, y el 82,93 % no, tuvieron este problema.

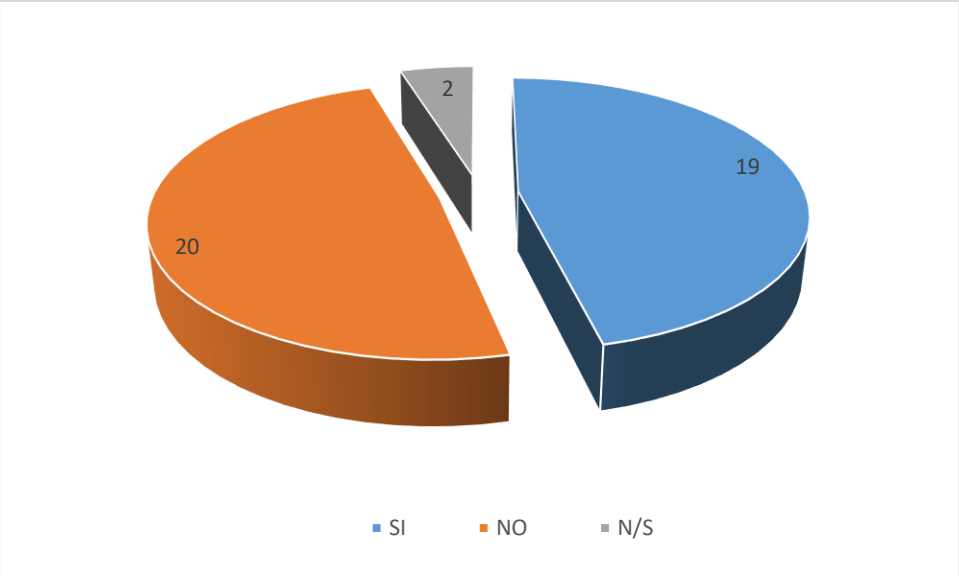
Tabla 9 "Seguridad en la estación de trabajo"

RESPUESTA	CANTIDAD	PORCENTAJE
SI	19	46,34%
NO	20	48,78%
N/S	2	4,88%
Total:	41	100%

Elaborado por: El autor

Fuente: encuesta in situ

Gráfico 7 “Seguridad en la estación de trabajo”



Elaborado por: El autor

Fuente: encuesta in situ

La encuesta muestra, en la pregunta siete, “¿Tiene Ud. seguridad en su estación de trabajo?”, se indica que el 46,34 por ciento de las personas encuestadas, tienen seguridad en su computador y el 48,78 por ciento, no tienen seguridad en sus pcs, por ende, tienen vulnerabilidades en la seguridad de sus datos.

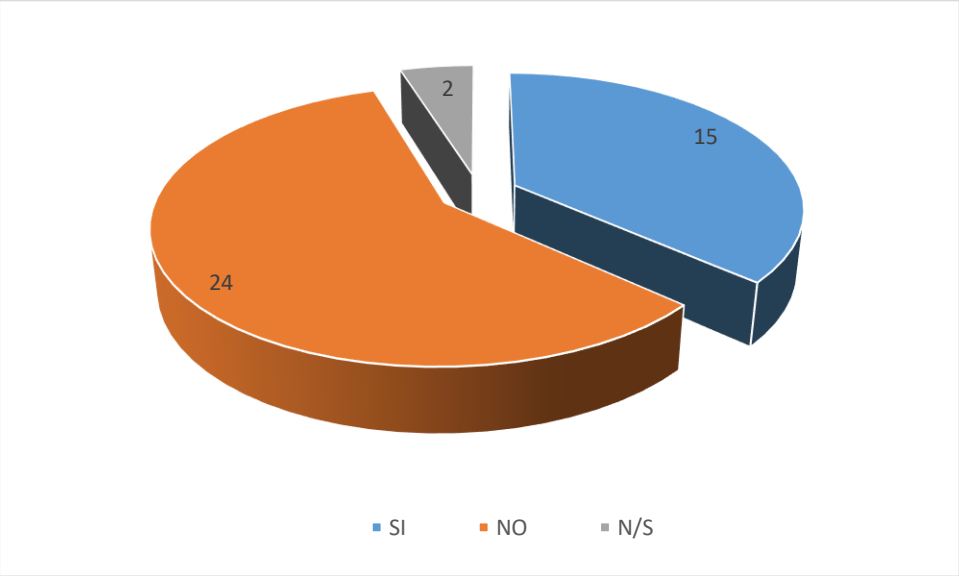
Tabla 10 "Antivirus en el teléfono celular"

RESPUESTA	CANTIDAD	PORCENTAJE
SI	15	36,59%
NO	24	58,54%
N/S	2	4,88%
Total:	41	100%

Elaborado por: El autor

Fuente: encuesta in situ

Gráfico 8 “Antivirus en el teléfono celular”



Elaborado por: El autor

Fuente: encuesta in situ

La encuesta muestra, en la pregunta ocho, “¿Tiene Ud. antivirus en su teléfono celular?”, se observa que el 58,54 % de las personas encuestadas, no tienen antivirus en su teléfono celular, por ende, tienen un problema de seguridad, en su celular personal.

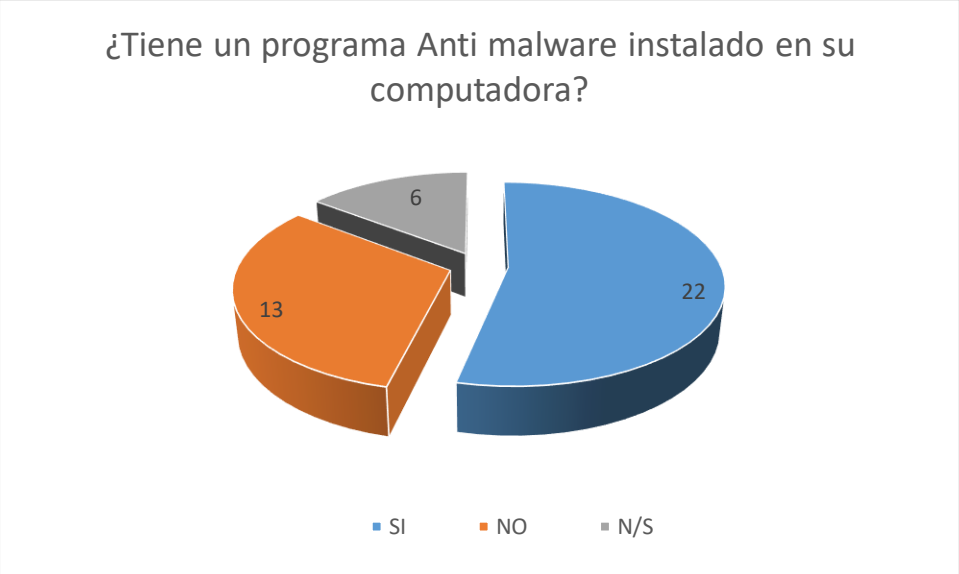
Tabla 11 "Anti malware instalado en su computadora"

RESPUESTA	CANTIDAD	PORCENTAJE
SI	22	53,66%
NO	13	31,71%
N/S	6	14,63%
Total:	41	100%

Elaborado por: El autor

Fuente: encuesta in situ

Gráfico 9 “Anti malware instalado en su computadora”



Elaborado por: El autor

Fuente: encuesta in situ

La encuesta muestra, en la pregunta nueve, “¿Tiene un programa Anti malware instalado en su computadora?”, se observa que el 31,71 % de las personas encuestadas, no tienen un anti malware en su computadora, por lo que están expuestos a ataques de tipo malware.

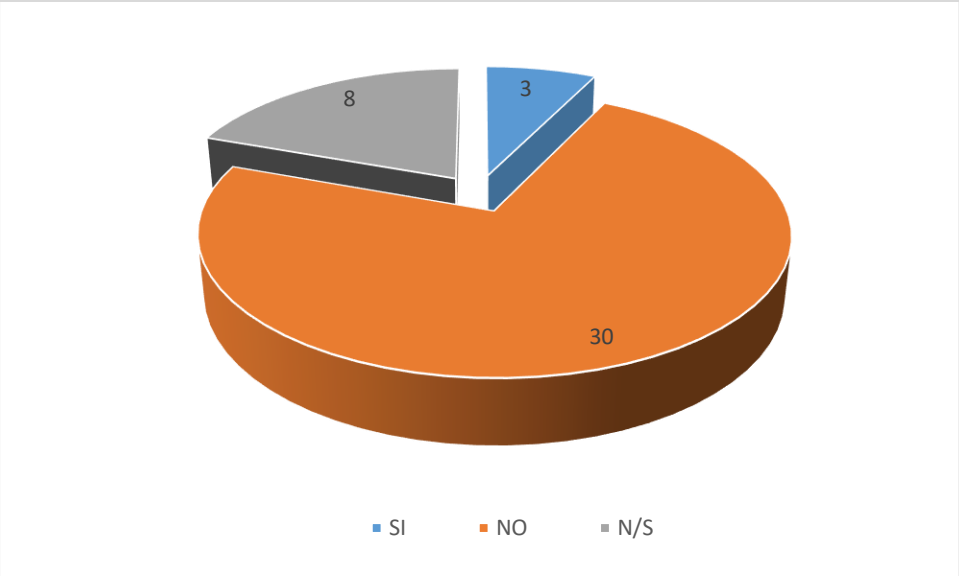
Tabla 12 "Consola de administración centralizada"

RESPUESTA	CANTIDAD	PORCENTAJE
SI	3	7,32%
NO	30	73,17%
N/S	8	19,51%
Total:	41	100%

Elaborado por: El autor

Fuente: encuesta in situ

Gráfico 10 “Consola de administración centralizada”



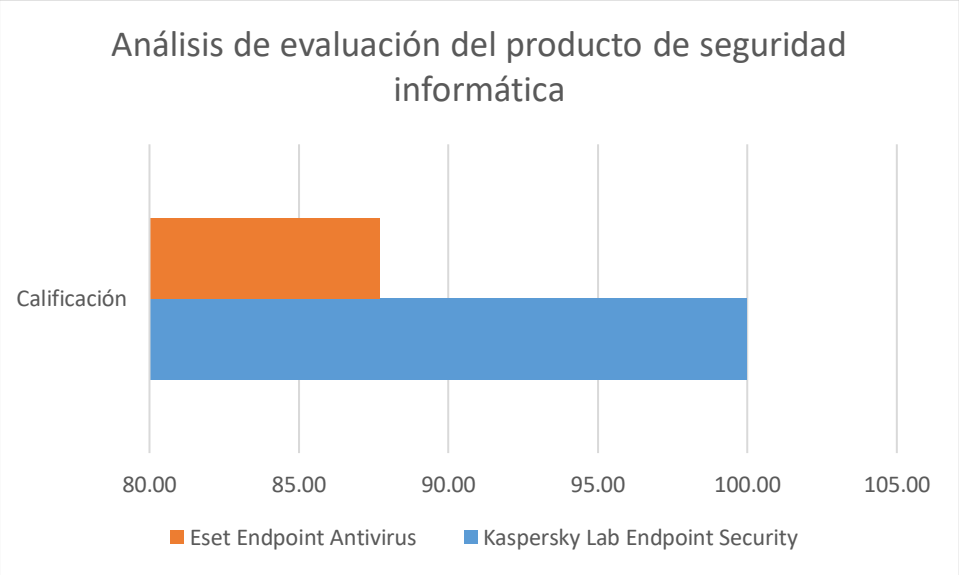
Elaborado por: El autor

Fuente: encuesta in situ

La encuesta muestra, en la pregunta uno, “¿Conoce Ud. ¿El uso de una consola de administración centralizada para todas las funciones, en su computadora?”, se indica que el 73,17 % de las personas encuestadas, no tienen un control, de monitoreo en su computador, el 7,32 % de las personas respondieron que sí, y el 19,51 % desconocen del tema.

4.0.2 Análisis del Ranking de herramientas de seguridad

Gráfico 11 “Calificación a las herramientas de seguridad informática”



Elaborado por: El autor

Fuente: encuesta in situ

Tabla 13 “Calificación a las herramientas de seguridad informática”

Producto	Calificación	Porcentaje
Kaspersky Lab Endpoint Security	100.00	100.00%
Eset Endpoint Antivirus	87.71	87.71%

Elaborado por: El autor

Fuente: encuesta in situ

La exploración, del Análisis de evaluación del producto de seguridad informática, muestra al Instituto AV-Test, especializado en test y certificaciones de antivirus, que califica, a la herramienta tecnológica empresarial de seguridad informática, Kaspersky Lab Endpoint Security, con una evaluación de 100/100, la cual es la máxima calificación, que existe en la actualidad, para este tipo de herramienta de seguridad informática.

4.1 Comprobación de la Hipótesis

De acuerdo a los resultados de la encuesta que se elaboró, se encuentra, que el 92,68% de los encuestados no tienen un antivirus de tipo empresarial. Y el 56,10% han tenido problemas de virus en sus computadoras. Lo que evidencia que existen problemas de vulnerabilidades en seguridad informática, en la empresa.

Se indica que el 17,07% de los encuestados, si han tenido ataques de captura de teclado, y el 63,41% no han tenido ataques de este tipo. Y el 48,78% personas encuestadas han encontrado archivos dañados en su computador.

El 29,27% de las personas encuestadas, han perdido información en su computadora. Y el 17,07% de encuestados encontró sus archivos, con información cambiada, en su equipo de computación.

Se observa que el 48,78% de las personas encuestadas no tienen, seguridad en su computadora. También encontramos que el 58,54% de los encuestados, no tiene un antivirus en su celular.

El 31,71% de las personas encuestadas, no tienen un programa anti malware en su computadora. Y el 73,17% de los encuestados, no tienen una consola de administración centralizada para monitorear el uso de su computadora. Esto evidencia un gran desconocimiento de la existencia de las herramientas de seguridad informática, y al desconocer, el usuario, no puede aplicar su utilización.

En la exploración hecha, a las empresas especializadas, de realizar test y certificaciones de antivirus, se indica que, el disponer de un sistema antivirus tipo empresarial, si protege los equipos de computación y la disponibilidad de la información, porque el Instituto especializado en test y certificaciones, AV-Test, dice que la herramienta de seguridad informática, Kaspersky Endpoint security, protege el 100%, de los

problemas de vulnerabilidades a la seguridad informática, en los equipos de computación.

Por ende, se comprueba la hipótesis con los resultados obtenidos, en la encuesta aplicada, y la exploración en documentos web realizada.

CAPITULO V

DISEÑO DE LA PROPUESTA

5.1 La Propuesta

En el presente capitulo se presenta una sugerencia, para minimizar las vulnerabilidades a la seguridad informática de la empresa Aguapen EP, en el año 2016, consiste en sugerir la adquisición e implementación de herramientas de seguridad informática, que cumplan con los estándares de seguridad informática, de tipo empresarial.

5.2 Objetivos de la Propuesta

5.2.1. Objetivo general de la Propuesta

Sugerir una solución a los problemas de seguridad de los datos y computadoras, usando herramientas tecnológicas para la seguridad informática en la empresa pública Aguapen EP

5.2.2 Objetivos específicos de la Propuesta

- Investigar cuales son las mejores herramientas tecnológicas para la seguridad informática
- Determinar cuál es la mejor herramienta tecnológica de seguridad informática, para los intereses financieros de la empresa, a nivel de costo

5.3 Estratégica de la propuesta

La estrategia de la propuesta, se diseña en “El plan para sugerir la mejor herramienta de seguridad informática”, con una duración de dos meses y todas las actividades se las realiza en la empresa Aguapen EP

Tabla 14 "Estratégica de la propuesta"

PLAN PARA SUGERIR LA MEJOR HERRAMIENTA DE SEGURIDAD INFORMÁTICA A LA EMPRESA AGUAPEN EP									
PROPUESTA	ACTIVIDADES PROGRAMADAS	TIEMPO DE DURACIÓN							
		PRIMER MES				SEGUNDO MES			
		SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 5	SEMANA 6	SEMANA 7	SEMANA 8
Diseñar una propuesta para minimizar los problemas de vulnerabilidades a la seguridad informática en la empresa Aguapen EP	a) Conocimiento del entorno in sitio								
	b) elaborar la encuesta								
	c) Ejecutar la encuesta								
	d) Recopilar la información de la encuesta								
	e) Tabular la información recopilada								
	f) Elaborar las tablas con los resultados								
	g) Elaborar los gráficos con los resultados								
	h) Investigar sobre herramientas Tecnológica de Seguridad Informática								
	i) Determinar la mejor herramienta de Seguridad Informática								
	j) Solicitar las cotizaciones de las Herramientas de Seguridad Informática								
	k) Sugerir la mejor herramienta de Seguridad Informática								
Periodo de ejecución Entrega y revisión del producto									

Elaborado por: El autor

El presente plan, se inicia con la observación del entorno de trabajo, en la empresa Aguapen EP, para conocer de cerca la situación inicial, en que se encuentran trabajando las computadoras, a nivel de seguridad informática.

Posteriormente se elabora una encuesta, con los problemas de seguridad informática, más comunes, existentes a la actualidad.

Ejecutamos la encuesta, para recabar la información e incidencia de los problemas de seguridad informática, que tiene el parque de computadoras de Aguapen EP.

Se recopila y tabula la información en Excel, agrupando los datos, según cada pregunta, para presentar un consolidado por cada respuesta.

Elaboramos las tablas y gráficos con los resultados de la encuesta tabulada en Excel, por cada pregunta.

Adicionalmente se investiga, en empresas especializadas del ranking, de las herramientas de antivirus a nivel empresarial, para conocer que evaluación tiene cada herramienta de seguridad informática.

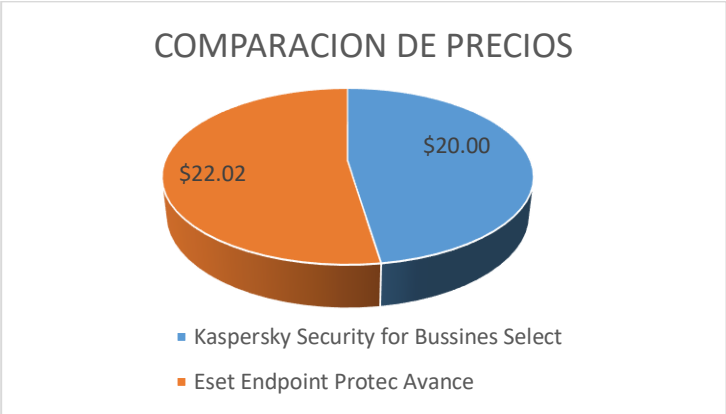
Haciendo un análisis, en base a la investigación del ranking de herramientas de seguridad informática, se determina la opción más conveniente para la empresa Aguapen EP.

Con toda esta información, del trabajo anteriormente descrito se procede, a elaborar la sugerencia, donde se determina la mejor herramienta de seguridad informática, según la conveniencia y necesidades de la empresa Aguapen EP

5.4 Comparación de Precios de las herramientas de seguridad

En base a la investigación del ranking de herramientas de seguridad informática, se selecciona dos empresas de seguridad, que tienen una evaluación buena en su desempeño y tienen oficinas representantes o distribuidores en el Ecuador, a continuación, se presenta, el comparativo de las cotizaciones, de las herramientas de seguridad informatica de las empresas Kaspersky y Eset.

Gráfico 12 Comparación de precios de las herramientas de seguridad informática



Elaborado por: El autor

Fuente: Kaspersky y Eset

Tabla 15 Comparación de precios de las herramientas de seguridad informática

COMPARACION DE PRECIOS	
HERRAMIENTA	**COSTO**
Kaspersky Security for Bussines Select	$20,00
Eset Endpoint Protec Avance	$22,02
Diferencia:	**$2,02**

Elaborado por: El autor

Fuente: Kaspersky y Eset

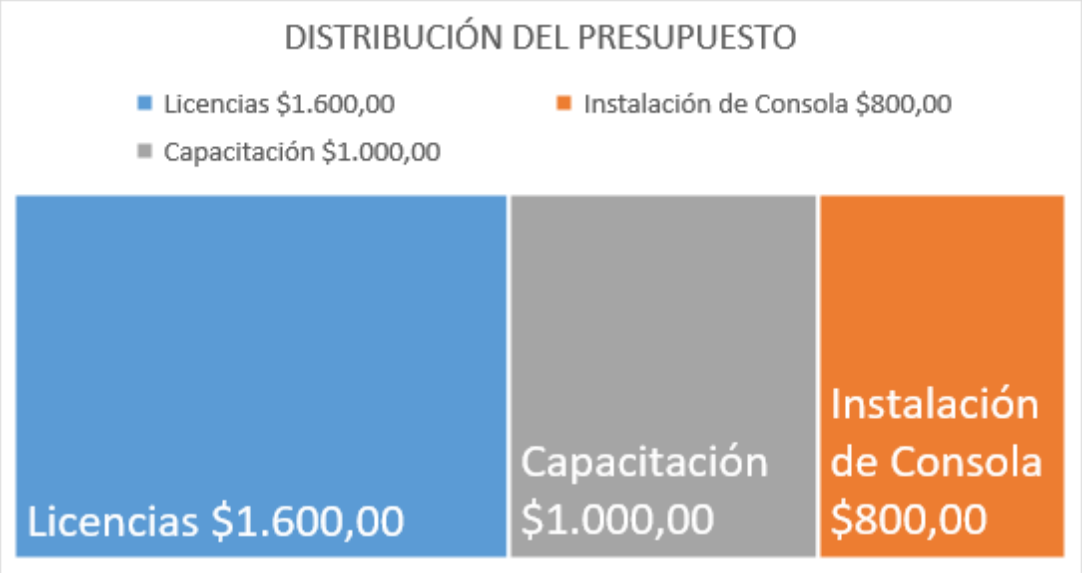
Como se puede observar en el gráfico 12, la empresa kaspersky vende su producto, Kaspersky Security for Bussines Select, en $20,00. Y la empresa Eset vende su producto, Eset Endpoint Protec Avance, en $22,02.

Adicionalmente en la tabla 15 podemos apreciar, que la herramienta de seguridad informática de la empresa Eset es más cara, que la herramienta que ofrece la empresa Kaspersky, con una diferencia de $2,02.

Esta diferencia multiplicada por 80 computadoras, da un resultado de $161,60 dólares americanos, por ende, a nivel financiero es más conveniente comprar la herramienta de seguridad informática de la empresa Kaspersky, en su producto, Kaspersky Security for Bussines Select.

5.5 Presupuesto de la Propuesta

Gráfico 13 "Presupuesto de la Propuesta"



Elaborado por: El autor

Fuente: encuesta in situ

Tabla 16 "Presupuesto"

PRESUPUESTO	
OPERACIÓN	**PRESUPUESTO**
Licencias	$1.600,00
Instalación de Consola	$800,00
Capacitación	$1.000,00
Total:	**$3.400,00**

Elaborado por: El autor

El costo de cada licencia de utilización por un año, de la herramienta tecnológica empresarial Kaspersky Endpoint security, es de $20.00 dólares americanos, por cada equipo de computación, en total se suma $1.600,00 dólares americanos, el costo de la instalación de la consola de monitoreo y 10 licencias in situ (con transferencia de tecnología), es de $800.00 dólares americanos y el costo de la capacitación para dos personas, es de $1.000,00 dólares americanos, que dan un total de $3.400,00 dólares americanos

Si no se compra esta solución a las vulnerabilidades de seguridad informática, las computadoras de la empresa Aguapen EP, están expuestas, a toda clase de ataques de virus, hackers y malware, por ende, se corre un alto riesgo, de perdida de información y daños en los equipos de computación. Estableciendo un costo promedio para cada equipo de computación de $1.000,00, y tomando en cuenta la cantidad de la muestra, de 41 computadoras, multiplicamos por su costo, los costos anuales en daños por virus y hackers, pueden alcanzar los $41.000,00. Dependiendo de la cantidad de ataques a los equipos de computación por personas, no autorizadas.

Si se hace la compra de las herramientas tecnológicas de seguridad informática, se evitará perdida de información, daños de los datos, averías en los equipos de computación, se impedirá infecciones de virus en las computadoras, se evitará que baje la producción, en el trabajo del personal administrativo, se obviará costos de reparación y reposición de los equipos de computación, salvaguardando un parque de computadoras, valorado en $80.000,00 dólares americanos.

Se recomienda la compra de las licencias de utilización, de la herramienta de seguridad informática tipo empresarial, por tres años, para bajar costos operativos, porque la empresa Kaspersky, vende su licencia de uso a tres años, a razón de $39.00 dólares americanos.

Adicionalmente se recomienda la compra e implementación de un servidor de dominio, para autentificar el acceso a la red de datos de la empresa, con el objetivo de evitar el acceso a la red de terceras personas, que no tienen autorización de utilizar la red de la empresa.

Conclusiones

- Se concluye, haciendo un análisis a la mejor calificación del ranking de evaluación a las herramientas de seguridad informática, como se aprecia en la tabla 13, y la herramienta de seguridad que tiene el precio más conveniente como se observa en el grafico 12, se establece que el producto Kaspersky Security for Bussines Select, de la empresa Kaspersky. Es el más conveniente para su compra e implementación, en la empresa Aguapen EP.
- Se concluye que los tipos más comunes de problemas de seguridad informática a nivel mundial, son el malware, virus, hackers, usuarios, programas maliciosos, errores de programación, intrusos, siniestros externos, personal técnico de la empresa, fallos eléctricos, como se puede apreciar en el capítulo 2.7 y según el National Institute of Standards and Technology
- Se concluye que las amenazas a la seguridad informática que se encontraron en la empresa Aguapen EP, como sugiere el capítulo 4.0.1, son:
    - Falta de un antivirus de tipo empresarial
    - Se reporta la existencia de virus en las computadoras
    - Falta de seguridad en la estación de trabajo
    - Los usuarios no tienen un antivirus en su celular
    - La empresa no tiene una consola de administración centralizada, para monitorear las actividades de las computadoras
- En conclusión, se sugiere la compra e implementación de la herramienta de seguridad informática de la empresa Kaspersky, con su producto, Kaspersky Security for Bussines Select

Recomendaciones

- Se recomienda elegir el programa de seguridad informática, que cumpla con la mayor puntuación en el ranking de herramientas de seguridad.
- Recomiendo, dar un especial monitoreo, a las principales amenazas de seguridad informática, que se encuentran actualmente, en el mundo, para minimizar los problemas, que estas amenazas conllevan.
- Se recomienda establecer la mejor solución en seguridad informática, también por su costo.
- Se recomienda poner especial énfasis, para solucionar los problemas de seguridad encontrados en el parque de computadoras de la empresa Aguapen EP, según lo expresa las normas Cobit 5
- Se recomienda el uso continuo de la herramienta de seguridad informática Kaspersky, con su consola de monitoreo centralizada.

Bibliografía

Abad-Aramburu, C. (2015). *http://reunir.unir.net.* Obtenido de Tesis de Masterado.

Abril, A. P. (10 de 04 de 2014). *http://www.revistasjdc.com*. Obtenido de Artículo científico: http://www.revistasjdc.com/main/index.php/rciyt/article/view/292

Aguapen-EP. (10 de 01 de 2016). *http://aguapen.gob.ec*. Obtenido de Misión & Visión: http://aguapen.gob.ec/index.php/2012-05-31-16-08-12/mision-vision

Aguapen-EP. (05 de 02 de 2016). *http://aguapen.gob.ec*. Obtenido de VALORES ESENCIALES: http://aguapen.gob.ec/index.php/2012-05-31-16-08-12/objetivos

ALVARADO, V. L. (10 de 01 de 2013). *http://s3.amazonaws.com/academia.edu.documents*. Obtenido de Tesis de grado: http://s3.amazonaws.com/academia.edu.documents/34539454/CD-4645.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1474500005&Signature=uq5neRD4fyPV3p2GU8u2V0DqqNE%3D&response-content-disposition=inline%3B%20filename%3DESCUELA_POLITECNICA_NACIONAL.pdf

Bártoli, C. G. (10 de 01 de 2012). *http://sedici.unlp.edu.ar*. Obtenido de Proyecto Academico: http://sedici.unlp.edu.ar/bitstream/handle/10915/19475/Documento_completo.pdf?sequence=1

Belloch, C. (10 de 02 de 2012). *http://www.uv.es*. Obtenido de Artículo cientifico: http://www.uv.es/bellochc/pedagogia/EVA1.pdf

Bermúdez Molina, K. G. (01 de 03 de 2015). *http://www.dspace.ups.edu.ec.* Obtenido de Tesis de grado: http://www.dspace.ups.edu.ec/handle/123456789/10372

Cecchini, R. L. (10 de 01 de 2015). *uns.edu.ar*. Obtenido de Tesis de Doctorado: http://repositoriodigital.uns.edu.ar/handle/123456789/2119

Condar Guisbert, A. P. (2014). Que tipo De virus esconde las paginas de la Deep Web. Revista de Información, Tecnología y Sociedad, 26. *Rebistas Bolivarianas*, 1.

Cuevas Martínez, R. (10 de 01 de 2012). *http://contenidosabiertos.academica.mx*. Obtenido de Artículo científico: http://contenidosabiertos.academica.mx/jspui/handle/987654321/503

De Alonso, M. C. (2016). Las matemáticas en la ingeniería a través de la historia. *Ciencia e Ingeniería Neogranadina, 13(1)*, 53-60.

EP, A. (10 de 01 de 2016). *http://aguapen.gob.ec*. Obtenido de Misión & Visión: http://aguapen.gob.ec/index.php/2012-05-31-16-08-12/mision-vision

ESTRADA ROJAS, S. R. (10 de 02 de 2016). *http://repositorio.ug.edu.ec*. Obtenido de Artículo científico: http://repositorio.ug.edu.ec/handle/redug/2533

Fernández, J. &. (2013). *Seguridad en Informática.* Mexico: Aprocal.

Fernández, L. G. (01 de 12 de 2012). *http://s3.amazonaws.com/academia.edu.documents*. Obtenido de Artículo científico:

http://s3.amazonaws.com/academia.edu.documents/36974512/NOV_DOC_Tabla_AEN_22994_1.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1474499338&Signature=Eq%2BMRwV3kSMB7jPA5t7iD53ygxY%3D&response-content-disposition=inline%3B%20filename%3DNOV_DOC_Tabla_AEN_2

Flórez, W. A. (2015). Solución integral de seguridad para las pymes mediante un UTM. *Revista Ingenierías USBMed*, 35-42.

Franco, D. A. (11 de 03 de 2012). *http://www.scielo.cl*. Obtenido de Artículo científico: http://www.scielo.cl/scielo.php?pid=S0718-07642012000300014&script=sci_arttext

Franco, D. A. (01 de 10 de 2013). *http://www.scielo.cl.* Obtenido de Articulo cientifico: http://www.scielo.cl/scielo.php?pid=S0718-07642013000500003&script=sci_arttext&tlng=e

Fritz, E. M. (07 de 06 de 2015). *http://sedici.unlp.edu.ar*. Obtenido de Artículo científico: http://sedici.unlp.edu.ar/handle/10915/46010

García, N. Y. (2012). IMPLEMENTACIÓN Y ACTUALIZACIÓN EN LA INFRAESTRUCTURA DE SEGURIDAD DE UNA RED INFORMÁTICA. *Redes de Ingeniería*, 21-31.

Grácia, A. P. (2013). ¿ Qué sabemos acerca del web malware?. *SIC: ciberseguridad, seguridad de la información y privacidad, (107)*, 104 - 106.

Hernández, W. G. (2016). La implementación de procesos de informatización en organizaciones como competencia en la formación de profesionales en informática. *e-Ciencias de la Información, 6(2)*, 18.

https://www.virusbulletin.com. (01 de 06 de 2016). *https://www.virusbulletin.com*. Obtenido de Ranking mundial: https://www.virusbulletin.com/testing/results/compare/vb100-antimalware/eset-nod32__vs__kaspersky-es/in-last-10-tests

ISACA. (2012). *COBIT 5, Un Marco de Negocio para el Gobierno y la Gestiónde las TI de la Empresa.* Rolling Meadows: COBIT.

Jara, H. &. (2012). *Ethical Hacking 2.0.* Madrid: Usershop.

López, A. B. (2014). Vulnerabilidad de Ambientes Virtuales de Aprendizaje utilizando SQLMap, RIPS, W3AF y Nessus [Vulnerability in Virtual Learning Environments using SQLMap, RIPS, W3AF and Nessus]. *Ventana Informática*, 30.

MARTIN, P. E. (24 de 07 de 2015). *http://www.ieee.es.* Obtenido de Artículo científico: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO79-2015_InseguridadCibernetica_AmericaLatina_PaulE.Martin.pdf

Martínez, Y. P. (10 de 11 de 2012). *http://publicaciones.uci.cu.* Obtenido de Artículo científico: http://publicaciones.uci.cu/index.php/SC/article/view/965

Monroy, M. E. (01 de 10 de 2012). *http://www.scielo.cl/*. Obtenido de Caracterización de Herramientas de Ingeniería Inversa: http://www.scielo.cl/scielo.php?pid=S0718-07642012000600005&script=sci_arttext&tlng=pt

Montesino Perurena, R. B. (2013). Gestión automatizada e integrada de controles de seguridad informática. *Scielo*, 40-58.

Oliva, J. &. (15 de 06 de 2014). *www.elastix.org*. Obtenido de Artículo Científico: http://blogs.elastix.org/wp-content/uploads/2015/04/Seguridad_en_Implementaciones_voip.pdf

Ovalle, D. A. (2014). Modelo de Recomendación Personalizada en Cursos Virtuales basado en Computación Ubicua y Agentes Inteligentes. *Inf. tecnol. vol.25 no.6 La Serena 2014*, 131-142.

Ovalle, S. O. (01 de 07 de 2012). *http://www.eumed.net*. Obtenido de Seguridad Informatica: http://www.eumed.net/rev/cccss/21/oocs.pdf

Portantier, F. (2012). *Seguridad informática.* Madrid: USERSHOP.

Semprini, G. &. (10 de 05 de 2013). *http://42jaiio.sadio.org.ar.* Obtenido de Artículo Científico: http://42jaiio.sadio.org.ar/proceedings/simposios/Trabajos/SID/17.pdf

Sisalima, O. &. (11 de 11 de 2015). *http://repositorio.utmachala.edu.ec*. Obtenido de Artículo científico: http://repositorio.utmachala.edu.ec/handle/48000/5157

Tarazona, G. M. (2013). BUENAS PRÁCTICAS PARA IMPLEMENTACIÓN DEL COMERCIO ELECTRÓNICO EN PYMES. *Visión Electrónica*, 31-45.

VARGAS, I. A. (20 de 04 de 2013). *http://www.isa-spain.org*. Obtenido de Artículo Científico: http://www.isa-spain.org/images/biblioteca_virtual/sesion%201a%5B1%5D.%20%23isa%20-%20ponencia%20conferencia%20anual%202007%20-%20seguridad%20en%20redes%20industriales.pdf

Vazquez, M. (. (10 de 12 de 2012). *https://dspace.palermo.edu*. Obtenido de Tesis de grado: https://dspace.palermo.edu:8443/xmlui/handle/10226/1483

Vieites, A. G. (10 de 12 de 2013). *http://www.edisa.com*. Obtenido de Articulo cientifico: http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

Villanova-Pascual, O. (17 de 05 de 2016). *reunir.unir.net.* Obtenido de Tesis de Masterado: http://reunir.unir.net/handle/123456789/3622

www.av-test.org. (01 de 04 de 2016). *www.av-test.org*. Obtenido de www.av-test.org: https://www.av-test.org/es/antivirus/empresas-windows-client/windows-10/abril-2016/kaspersky-lab-endpoint-security-10-161537/

ANEXOS
CARTA A LA UNIDAD DE OBSERVACIÓN

www.uteg.edu.ec

UTEG
UNIVERSIDAD TECNOLÓGICA EMPRESARIAL DE GUAYAQUIL

Guayaquil, 30 de Septiembre del 2016

Señor:
Ing. Gino Farfán
GERENTE GENERAL
Empresa Pública Municipal Mancomunada Aguapen EP
Ciudad. -

De mis consideraciones:

Reciba un cordial saludo de quienes conformamos la **Universidad Tecnológica Empresarial de Guayaquil – UTEG.** El propósito de la presente es, solicitarle a usted, permita que la alumno **William Marcelo Rodríguez Plaza, CI. # 0913912762** quien se encuentra realizando su Trabajo de Titulación pueda visitar las instalaciones de vuestra Empresa con el afán de obtener la información necesaria que complemente su trabajo de tesis cuyo tema titula:
"ANÁLISIS DE VULNERABILIDADES A NIVEL DE SEGURIDAD INFORMÁTICA EN EL PARQUE COMPUTACIONAL DE AGUAPEN EP. EN EL 2016"

Esperando contar con una respuesta favorable a nuestra solicitud, como así también, en caso de ser aprobada, tener a bien informarnos la fecha y el horario en que se podría realizar la visita agradeciendo desde ya la atención dispensada.

AGUAPEN-EP
05 OCT 2016
Shayna P.

06/10/2016. 10:41

Atentamente,

Dr. José Bohórquez Zavala
Decano de Grado

UTEG
DECANATO

Urdesa Central
Guayacanes 520 y calle 5ta
Tel: (593) 042884833
Guayaquil - Ecuador

AUTORIZACIÓN

Aguapen-EP
Empresa Pública Municipal Mancomunada

G.A.D.M SALINAS G.A.D.M SANTA ELENA G.A.D.M LA LIBERTAD

OFICIO N°AGUAPEN-GG-0684-2016
Oficina Matriz, Salinas 07 de octubre de 2016

Asunto: Autorización para trabajo de titulación.

Doctor
José Bohórquez Zavala
Decano de Grado
Universidad Tecnológica Empresarial de Guayaquil
Guayaquil.-

De mi consideración:

Reciba un cordial saludo de quienes conformamos la Empresa Pública Municipal Mancomunada De Los Gobiernos Autónomos Descentralizados Municipales De Los Cantones Santa Elena, Salinas y La Libertad Para El Servicio Público De Agua Potable, Alcantarillado Sanitario, Pluvial, Depuración Y Aprovechamiento De Aguas Residuales De Las Zonas Urbanas y Rurales De Los Cantones De La Provincia De Santa Elena AGUAPEN-E.P., deseándole el mayor de los éxitos en sus funciones que acertadamente dirige.

En atención al Oficio S/N suscrito por usted y recibido en las instalaciones de nuestra oficina matriz el día jueves 06 del presente mes y año, solicitando que se brinde permiso para visitar las instalaciones de nuestra empresa, al estudiante **William Marcelo Rodríguez Plaza** para obtención de información para el desarrollo de su propuesta tecnológica **"Análisis de vulnerabilidades a nivel de seguridad informática en el parque computacional de AGUAPEN E.P en el 2016"** siendo este un requisito indispensable para la obtención del título de Ingeniero en Sistemas, debo manifestarle que:

En vista del esfuerzo, empeño, sacrificio y dedicación a los estudios universitarios del estudiante **William Marcelo Rodríguez Plaza** y con el afán de aportar a la obtención del título de tercer nivel esta gerencia **aprueba** su petición.

Particular que comunico a usted para los fines pertinentes.

Atentamente,

Ing. Gino Farfán Pazos
Gerente General

C.c: José Ramírez Ortega - **Jefe Del Departamento De Tecnologías De La Información**
Lcda. Karen Ochoa Tumbaco - **Directora De Talento Humano**

Archivo
GFP/GMM

Nota: Para coordinar el inicio de la recopilación de datos se encuentra habilitado el número de teléfono convencional (04)2775439, con el Sr. José Ramírez Ortega en la ext. 159.

1

EL AGUA ES PROGRESO
Número telefónico PBX: 2775439 Email: aguapen@aguapen.gob.ec
Oficina Matriz: Calle Costa de Oro, Calle 3, Av. 11 Mz *5, diagonal al conjunto residencial "Los Arenas"

FOTOS


CAJA 1
CAJA 2

CUESTIONARIO DE PREGUNTAS

1.- ¿Su computadora tiene instalado un antivirus de tipo empresarial?

Si ☐ No ☐ N/S ☐

2.- ¿Su computadora ha tenido problemas de virus?

Si ☐ No ☐ N/S ☐

3.- ¿Su equipo de computación ha tenido ataques de captura de teclado?

Si ☐ No ☐ N/S ☐

4.- ¿Usted ha encontrado archivos dañados en su computador?

Si ☐ No ☐ N/S ☐

5.- ¿Usted ha tenido perdida de información?

Si ☐ No ☐ N/S ☐

6.- ¿Usted ha encontrado archivos, con la información cambiada?

Si ☐ No ☐ N/S ☐

7.- ¿Tiene Ud. seguridad en su computadora de trabajo?

Si ☐ No ☐ N/S ☐

8.- ¿Tiene Ud. Antivirus en su teléfono celular?

Si ☐ No ☐ N/S ☐

9.- ¿Tiene un programa Anti malware instalado en su computadora?

Si ☐ No ☐ N/S ☐

10.- ¿Conoce Ud. ¿El uso de una consola de administración centralizada para todas las funciones, en su computadora?

Si ☐ No ☐ N/S ☐

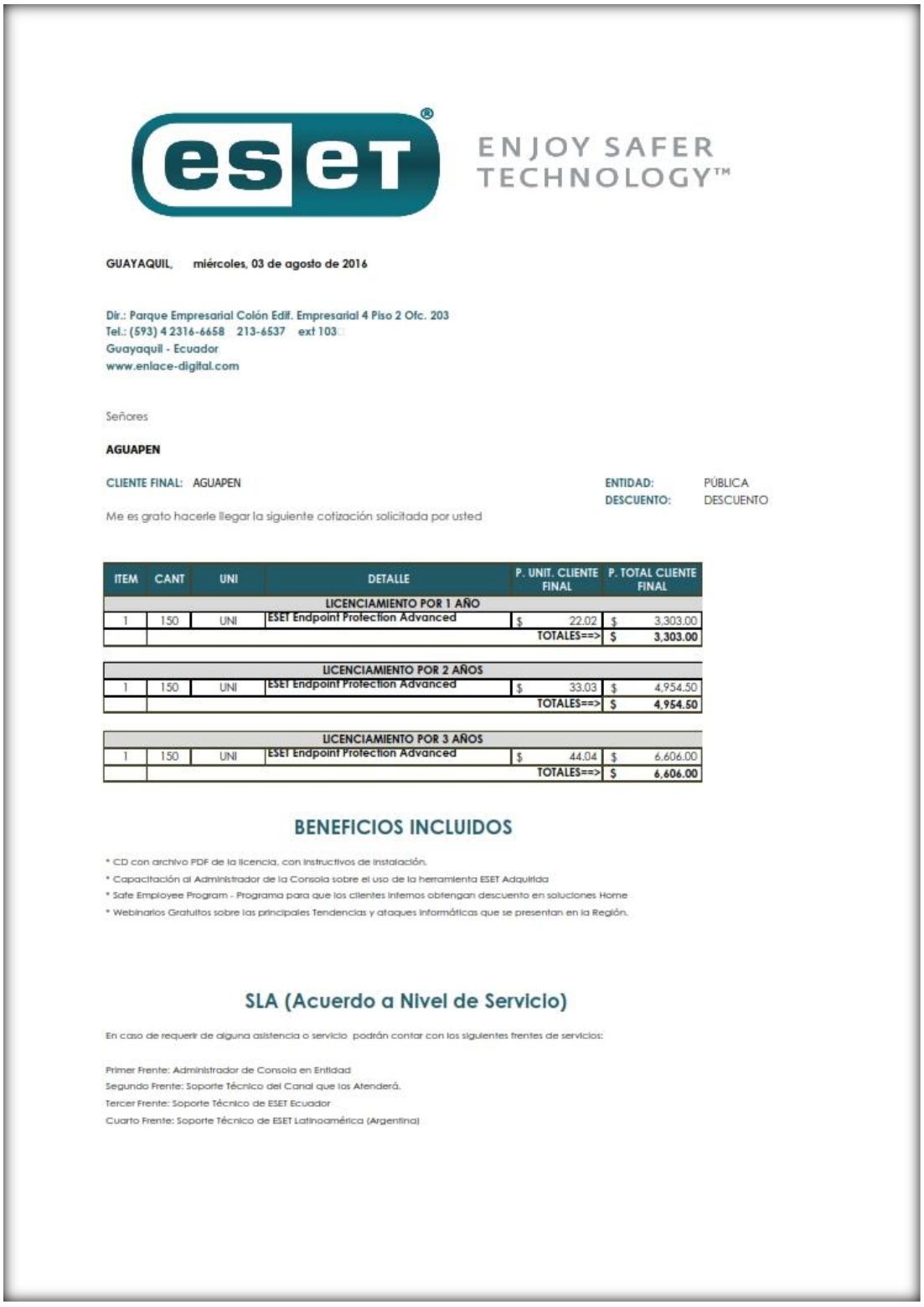
COTIZACIÓN KASPERSKY

IV. Propuesta Económica

Descripción	CANTIDAD	TOTAL 1 año	TOTAL 2 años	TOTAL 3 años
KASPERSKY SECURITY FOR BUSINESS - SELECT				
20 Licencias para protección de estaciones de trabajo mas una licencia para servidor servidor.	200	$ 20,00	$ 28,00	$ 39,00
El servicio incluye:				
Características principales				
Control de dispositivos mobiles				
Protección de Internet				
Seguridad para dispositivos móviles				
Control Web				
Control de Aplicaciones				
Control de dispositivos				
Lista Blanca De aplicaciones				
SERVICIOS PROFESIONALES				
Instalacion en consola y 10 estaciones de trabajo en sitio, transferencia de conocimientos.	1	$ 800,00	$ 800,00	$ 800,00
TOTAL		4.800	6.400	8.600

Descripción	CANTIDAD	TOTAL 1 año	TOTAL 2 años	TOTAL 3 años
KASPERSKY SECURITY FOR BUSINESS - ADVANCED				
20 Licencias para protección de estaciones de trabajo mas una licencia para servidor servidor.	200	$ 26,00	$ 39,00	$ 52,00
El servicio incluye:				
Características principales:				
Control de dispositivos mobiles				
Protección de Internet				
Seguridad para dispositivos móviles				
Control Web				
Cifrado de Datos				
Manejo de Parches				
Inventario de HW / SW				
Escaner de Vulnerabilidades Avanzado				
Configuracion y Despliegue de Sistemas				
Control de Aplicaciones				
Control de dispositivos				
Lista Blanca De aplicaciones				
SERVICIOS PROFESIONALES				
Instalacion en consola y 10 estaciones de trabajo en sitio, transferencia de conocimientos.	1	$ 800,00	$ 800,00	$ 800,00
TOTAL		6.000	8.600	11.200

COTIZACIÓN ESET



ENJOY SAFER TECHNOLOGY™

GUAYAQUIL, miércoles, 03 de agosto de 2016

Dir.: Parque Empresarial Colón Edif. Empresarial 4 Piso 2 Ofc. 203
Tel.: (593) 4 2316-6658 213-6537 ext 103
Guayaquil - Ecuador
www.enlace-digital.com

Señores

AGUAPEN

CLIENTE FINAL: AGUAPEN

ENTIDAD: PÚBLICA
DESCUENTO: DESCUENTO

Me es grato hacerle llegar la siguiente cotización solicitada por usted

ITEM	CANT	UNI	DETALLE	P. UNIT. CLIENTE FINAL	P. TOTAL CLIENTE FINAL
			LICENCIAMIENTO POR 1 AÑO		
1	150	UNI	**ESET Endpoint Protection Advanced**	$ 22.02	$ 3,303.00
				TOTALES==>	**$ 3,303.00**

			LICENCIAMIENTO POR 2 AÑOS		
1	150	UNI	**ESET Endpoint Protection Advanced**	$ 33.03	$ 4,954.50
				TOTALES==>	**$ 4,954.50**

			LICENCIAMIENTO POR 3 AÑOS		
1	150	UNI	**ESET Endpoint Protection Advanced**	$ 44.04	$ 6,606.00
				TOTALES==>	**$ 6,606.00**

BENEFICIOS INCLUIDOS

* CD con archivo PDF de la licencia, con instructivos de instalación.
* Capacitación al Administrador de la Consola sobre el uso de la herramienta ESET Adquirida
* Safe Employee Program - Programa para que los clientes internos obtengan descuento en soluciones Home
* Webinarios Gratuitos sobre las principales Tendencias y ataques informáticos que se presentan en la Región.

SLA (Acuerdo a Nivel de Servicio)

En caso de requerir de alguna asistencia o servicio podrán contar con los siguientes frentes de servicios:

Primer Frente: Administrador de Consola en Entidad
Segundo Frente: Soporte Técnico del Canal que los Atenderá.
Tercer Frente: Soporte Técnico de ESET Ecuador
Cuarto Frente: Soporte Técnico de ESET Latinoamérica (Argentina)