UNIVERSIDAD NACIONAL

JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

ESCUELA DE POSGRADO

TESIS

PRESENTADO POR:

MENA BERNAL HECTOR ANGEL

PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS

ASESOR:

DR. HUAMAN TENA ANGEL

HUACHO - 2019

APLICACIÓN DE PENTESTING Y PREVENCIÓN DE ATAQUES A LOS SISTEMAS DE INDUSTRIAS SAN MIGUEL DEL SUR – PLANTA HUAURA, AÑO 2019

MENA BERNAL HECTOR ANGEL

TESIS DE MAESTRÍA

ASESOR: DR. HUAMAN TENA ANGEL

UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN
ESCUELA DE POSGRADO
MAESTRO EN INGENIERÍA DE SISTEMAS
HUACHO

2019

DEDICATORIA

Dedico a mis padres, hermanos y seres queridos por su apoyo incondicional para hacer realidad esta investigación

Héctor Angel Mena Bernal

AGRADECIMIENTO

A mi Asesor de Tesis Dr. Ángel Huamán Tena, por su buena orientación y apoyo en el desarrollo de esta investigación.

Héctor Ángel Mena Bernal

ÍNDICE

INDICE TABLAS

INDICE FIGURAS

RESUMEN

Industrias San Miguel del Sur cuenta con 2 plantas (Huara y Arequipa) de embotellamientos dedicada a la producción de SOFTDRINK entre las marcas más destacadas (Agua Cielo, KR ,360 EnrgyDrink ,Sline , Drink-T, Kero y Fruvi cuenta con varias soluciones informáticas que permite la automatización de diferentes procesos que tenemos en el sistema Fox Pro , SAP y Sistema CNT. Todos estos Sistemas forman parte del Core del negociodesde el inicio del proceso de producción, transporte y distribución del producto a los centrosoperativos, tanto nacional como internacionalmente. Estos sistemas si bien es cierto se ha vuelto una plataforma de facto en Industrias San Miguel, ya que si uno de los sistemas tuviese una caída se paralizarían los procesos Core del negocio generando grandes pérdidas económicas a la organización.

Esto provoca una necesidad de disponer de una metodología para gestionar la seguridad que se pueda aplicar en los diferentes frentes de la corporación Industrias San Miguel del Sur-Planta Huaura. Además, con el fin de facilitar el trabajo a los responsables de cada proyecto, esta metodología ha de cubrir todas las fases del ciclo de vida que componen un proyecto.

Por lo antes expuesto el **Objetivo**: determinar la relación entre la aplicación de Pentesting y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019, **Métodos**: la Población es de 30 trabajadores de TI Industrias San Miguel del Sur. Considerándose como dimensión: Configuración, Pruebas de caja negra, criptografía, actualización, preventor, administración de privilegios, **Resultados**: los resultados muestran que la mayoría de los colaboradores si están de acuerdo con la aplicación Pentesting para la prevención de ataques a los sistemas. **Conclusiones**: se concluye que La Metodología Pentesting, se relaciona significativamente con los Sistemas de Industrias San Miguel del Sur con una alta correlación con un coeficiente de Spearman igual a 0.766 el análisis de p valor o Asintótica (Bilateral) = 0.000 que es menor que 0.05

Palabras clave**:** Pentesting, Ethical Hacking, Sistemas Prevención

ABSTRACT

Industrias San Miguel del Sur has 2 bottling plants (Huara and Arequipa) dedicated to the production of SOFTDRINK among the most prominent brands (Agua Cielo, KR, 360 EnrgyDrink, Sline, Drink-T, Kero and Fruvi has several IT solutions that allows the automation of different processes that we have in the Fox Pro, SAP and CNT system. All these systems are part of the core of the business from the beginning of the production, transportation and distribution process of the product to the operating centers, both National and Internationally, these systems, although it is true, have become a de facto platform in Industrias San Miguel since if one of the systems had a crash, the core business processes would be paralyzed, generating large economic losses to the organization.

This causes a need for a methodology to manage security that can be applied on the different fronts of the corporation Industrias San Miguel del Sur Planta Huaura. In addition, in order to facilitate the work of those responsible for each project, this methodology has to cover all phases of the life cycle that make up a project.

For the aforementioned, the Objective: to determine the relationship between the application of pentesting and the prevention of attacks on the systems of Industrias San Miguel del Sur - Huaura Plant, year 2019.Methods: The Population is 30 IT workers. Industrias san miguel del sur . Considering as dimension: Configuration, Black box tests, cryptography, update, preventor, privilege administration Results: the results show that the majority of the collaborators do agree with the pentesting application for the prevention of attacks on the systems. Conclusions: it is concluded that the Pentesting Methodology is significantly related to the San Miguel del Sur Industry Systems with a high correlation with a Spearman coefficient equal to 0.766 the analysis of p value or Asymptotic (Bilateral) = 0.000 which is less than 0.05

Keywords: Pentesting,Ethical Hacking, Prevention Systems

INTRODUCCIÓN

Actualmente el creciente uso masivo de la tecnología y de Internet ha facilitado al mundo,a ser parte de nuestro Core de negocio, soluciones informáticas de diferentes tipos de arquitecturas para diferentes procesos y áreas como lo es Administración, Producción y Transporte.

Puesto que algunos de estos servicios manejan información confidencial, es de vital importancia manejar dicha información con sumo cuidado, para evitar la pérdida, la manipulación, o que accedan a estos activos.

Debido a que los diferentes servicios mencionados antes, generalmente están automatizados mediante herramientas como las bases de datos, es de vital importancia asegurar estas herramientas para que en lo posible las intrusiones y manipulación sean nulas.

Este trabajo consistió en realizar una metodología que nos permita revisar y aumentar la seguridad en las aplicaciones desde varios frentes como preventivo y reactivo, el estudio comprende.

En el capítulo I, se desarrolla el marco de la realidad problemática formulada sobre las bases de revisiones bibliográficas, estudios exploratorios y técnicas apropiadas para el enfoque del problema.

En el capítulo II, en el marco teórico, se puntualiza sobre la institución en estudio y se indican estudios nacionales y extranjeros que fueron considerados; del mismo modo se exteriorizan las bases teórico-científicas de las variables enfocadas, que forman parte del soporte del estudio.

En el capítulo III, denominado marco metodológico, se especifican los elementosprimordiales del protocolo de investigación como: hipótesis, variables, tipo de investigación, diseño, método de estudio, población y muestra, técnicas de acopio de datos y método de análisis de datos.

En el capítulo IV, se presentan los resultados, como la aplicación de la metodologia de Pentesting, su valoracion de riesgos; asi mismo tenemos los análisis estadísticos, aquellos alcanzan la validación de instrumentos y la confiabilidad, como también la presentación de cuadros e interpretación de los resultados estadísticos y por último hacemos la contrastación de hipótesis.

En el capítulo V, parte final del trabajo de investigación se expresan de forma precisa las conclusiones más notables, se bosquejan recomendaciones a los directivos y a personas implicadas en el saber tecnológico, y también se adjuntan las evidencias en la sección de anexos que contribuyen a conseguir la credibilidad del estudio.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la realidad problemática

Desde el surgimiento de nuevas tendencias tecnológicas nos damos cuenta de que paralelamente fluctúan bugs o fallos. Aunque, en un sentido más amplio, también pueden ser el resultado de las propias limitaciones tecnológicas, porque, en principio, no existe un sistema 100% seguro. Por lo tanto, existen vulnerabilidades reales, conocidas como exploits. Los exploits son programas informáticos maliciosos (malware) que intentan utilizar y sacar provecho de un bug o vulnerabilidad en otro Software o sistema. Actualmentese encontró problemas de lentitud en el servidor web del site oficial de la empresa, el jefe de sistemas manifiesta que hubo acontecimientos inusuales que se repiten constantemente como la alteración en los registros contables en los sistemas core del negocio, sospecha que alguienestá manipulando el servidor web, por la lentitud y caídas constantes de la red interna eso permite evidenciar posibles ataques reales a la organización.

Industrias San Miguel-Planta Huaura, es una empresa que tiene como actividad principal la fabricación y comercialización de bebidas gasificadas saborizadas, aguas de mesa gasificadas y no gasificadas; aguas gasificadas saborizadas baja en calorías; bebidas saborizadas; bebidas de fruta adicionadas de vitaminas; bebidas gasificadas con cafeína; bebidas de té y bebidas de té bajo en calorías envasados en PET y vidrio, en sus 5 líneas de producción.

Incidentes que evidencia fue un ataque por un hacker de sombrero negro logrando la supresión de los bosques de usuarios del active directory de la red interna servidor basadaen tecnología Microsoft, de la Planta Huaura y dejando inoperativo 12 horas no solo a las oficinas sino también a los sistemas internos que manejan el personal administrativo y personal de producción esto afecta el día a día del personal operativ, como administrativo

respectivamente, impactando en la interrupción de procesos interno de la organización dejando inoperativo los accesos de las máquinas de producción sin poder producir nuestros productos como es el proceso de embotellamiento.

Han incrementado las vulnerabilidades al transcurrir los años de una maneraexponencial ya que la violación de integridad de la información dentro del organismo fue otra incidencia; asimismo hubo otro problema que fue la eliminación de la base de datos, en la cual se almacenaba dentro de la distribución de uno de nuestros sistemas informático interno, la investigación de la cartera de clientes para el proceso de preventa generando pérdidas económicas al eliminar información sensible como datos de la cartera de clientes como la dirección, correo electrónico, telefonía, entre otros. El hecho de volver a reconstruir la información genera un gasto y al mismo tiempo el no contar con los clientes realizar el proceso de ventas para la distribución de esta misma sin la dirección o datos completos del cliente; genera pérdidas económicas poniendo a la organización en proceso de riesgo en cuanto a su reputación en el mercado al no realizar los pedidos en el proceso de venta y entrega de la mercadería.

Nace la necesidad buscar una solución a dichos problemas informáticos manifestados anteriormente estas pérdidas económicas impactan en los estados financieros al cierre de año, como la utilidad utilidad neta. El interés de los hackers al dejar inoperativo los sistemas y al personal al no cumplir sus funciones operativas diarias como el registro y movimiento de cada producto. Tomando en cuenta que es una planta de producción de softdrink se necesita la disponibilidad de los sistemas informáticos las 24 hrs. por 7 días de la semana ya que hay un cronograma de producción y el hecho de parar produce grandes pérdidas económicas al no cumplir con la entrega de los productos a nuestros clientes, tanto nacional como internacionalmente.

1.2 Formulación del problema

1.2.1 Problema general

¿Qué relación existe entre la aplicación de Pentesting y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019?

1.2.2 Problemas específicos

a) ¿Qué relación existe entre la configuración y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019?

b) ¿Qué relación existe entre la prueba de caja negra y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019?

c) ¿Qué relación existe entre la prueba de criptografía y la prevención de ataques a los sistemas de Industrias San Miguel del Sur – Planta Huaura, año 2019?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Determinar la relación entre la aplicación de Pentesting y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019.

1.3.2 Objetivos específicos

a) Determinar la relación entre la configuración y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019.

b) Determinar la relación entre la prueba de caja negra y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019.

c) Determinar la relación entre la prueba de criptografía y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019.

1.4 Justificación de la investigación

Por medio del empleo de la aplicación de Pentesting es posible detectar el nivel de seguridad de los Sistemas de Información de Industrias San Miguel del Sur- Planta Huaura, ello se obtiene estableciendo el nivel de accesibilidad el cual un atacante obtendría con propósitos malintencionados a los sistemas informáticos desde la parte ofensiva.

Las pruebas de la metodología Ethical hacking son un paso previo a los análisis de fallas de seguridad o riesgos para una organización.

Son un camino precedente las pruebas de la metodología Ethical hacking a los análisis de fallas de seguridad o riesgos para una entidad.

Dejan despejado a las vulnerabilidades dichas pruebas el cual lograrán ser distinguidas y aprovechadas por sujetos no acreditados y extraños a la averiguación ya sea: hackers, crackers, ladrones, colaboradores existentes descontentos, ex-colaboradores, adversarios, etc. se encuentran completamente vinculados las pruebas de penetración, con el prototipo de averiguación que opera cada corporación, por ende, de acuerdo a la averiguación que se ansía resguardar, se establece las herramientas de seguridad y la estructura, sin embargo, de ningún modo al inverso. Se puede mencionar cuatro enfoques de justificación:

Económica

La empresa Industrias San Miguel del Sur - Planta Huaura, va a reducir sus costos al no haber pérdida de información ante un ataque informático.

Técnica

La ineludible tecnología para así desarrollar la aplicación de Pentesting, se localiza como utilizable dentro del mercado y se logra emplear, generando una cultura de seguridad de la información.

Operativa

Cuenta la empresa con colaboradores con conocimientos de tecnología de la información, quienes para el empleo de pruebas de penetración serían los soportes.

Personal

Accederá a que profundice el investigador dentro de los temarios concernientes al empleo de Pentesting y del mismo modo permitirá al investigador a conseguir su grado de maestro.

1.5 Delimitaciones del estudio

Delimitación Espacial

La presente investigación pretende determinar de qué manera la aplicación de Pentesting se relaciona con la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, ubicado en el Distrito de Huaura, Provincia de Huaura, Departamento de Lima, año 2019.

Delimitación Temporal

Se realiza el estudio dentro del periodo año 2019, conforme al cronograma establecido para la realización del estudio.

La empresa Industrias San Miguel del Sur – Planta Huaura cuenta con varias plantas de producción a nivel nacional e internacional y no se pudo trabajar en su totalidad con todas las plantas de producción. Se solicitó la autorización para trabajar en la planta de producción de Huaura donde el personal de la oficina de informática estuvo constituido por 30 trabajadores.

1.6 Viabilidad del estudio

Llevar a cabo el estudio fue posible ya que la población en esta oficina tiene las características disponibles a colaborar y para llevar a cabo los respectivos ensayos de esta manera se pudo obtener resultados fiables a partir de dichos estudios. Por lo tanto, la presenteinvestigación fue viable, por los siguientes motivos.

Recursos humanos. Se contó con la participación del investigador decidido en ejecutar la presente investigación por tratarse de su línea de investigación y por laborar en dicha empresa. Igualmente se contó con el apoyo de los directivos y la predisposición de los trabajadores de la Oficina de informática de la Empresa Industrias San Miguel del Sur – Planta Huaura en contestar las encuestas.

Recursos económicos. Para el presente estudio el investigador contó con recursos económicos para llevar a cabo la investigación, es decir se tuvo la capacidad de autofinanciar el costo de la investigación.

Recursos materiales. Se contó con todos los recursos materiales para llevar a cabo esta investigación.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes de la investigación

Actualmente estamos en la era donde la información se ha vuelto la materia prima de una organización y en cualquier ámbito de nuestra vida, las empresas poco a apoco se están concientizando sobre la importancia de la información que es valiosa y delicada. De la gran cantidad de estudios respecto a la seguridad informática, se pueden destacar los estudios mencionados a continuación.

2.1.1 Investigaciones internacionales

Verdesoto A. (2007). "Utilización de hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones" en la Escuela Politécnica Nacional, Ecuador.

Objetivo:

1) Determinar la integridad utilización de hacking ético para diagnosticar la seguridad de la Intranet de comunicaciones.

2) Determinar la disponibilidad utilización de hacking ético para diagnosticar la seguridad de la Intranet de comunicaciones.

3) Determinar la confidencialidad utilización de hacking ético para diagnosticar la seguridad de la Intranet de comunicaciones.

Metodología: Investigación no experimental, nivel de investigación Correlacional

Conclusiones:

Se desarrolla originariamente una introducción al extenso temario del Hacking Ético, precisando su empleo y las principales terminologías, conjuntamente se precisan en redes informáticos los principales mecanismos de la seguridad. Se les clasifica e ingresa al ambiente de los Hackers, se opina de como un Hacker malintencionado actúa, y las formas viables de un proceso de Hacking Ético. Para la ejecución de pruebas.

Como solución el Hacking ético aparece como una parte de una solución potencial para la seguridad en internet que se encuentra quebrantada, las cuales tiene un largo historial de éxito para muchos casos, pero también es cierto que esta técnica no es la única que se debe utilizar para asegurar la red.

Huilca. G. (2009). "Hacking ético para detectar vulnerabilidades en los servicios de laintranet del gobierno autónomo descentralizado municipal del cantón Cevallos" Para Optar el título Profesional de Ingeniero Informático y sistemas Escuela Politécnica Ambato Nacional, Ecuador,

Objetivo:

1) Determinar la integridad del Hacking ético para detectar vulnerabilidades en los servicios de la intranet del gobierno autónomo descentralizado municipal del cantón Cevallos

2) Determinar la disponibilidad del Hacking ético para detectar vulnerabilidades en los servicios de la intranet del gobierno autónomo descentralizado municipal del cantón Cevallos.

3) Determinar la confidencialidad del Hacking ético para detectar vulnerabilidades en los servicios de la intranet del gobierno autónomo descentralizado municipal del cantón Cevallos

Metodología: diseño de investigación no experimental, nivel de investigación Correlacional

Conclusiones:

Consiste un proyecto de Hacking Ético en una incursión registrada dentro de los sistemas informáticos de una corporación, del mismo modo que un pirata informático o hacker lo desarrollaría, sin embargo, de manera ética, previo permiso, por ende aconsejar las más adecuadas soluciones para cada uno de ellos. Por tal razón es sumamente significativo para detectar vulnerabilidades usando una revisión de Hacking Ético dentro de los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos, en tal sentido, se muestra una investigación el cual nos permitirá a tiempo descubrir las existentes vulnerabilidades, ofrecer viables soluciones y así procurar en asegurar las prestaciones y por ello lograr favorecer al Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos ofreciendo así seguros unos servicios y de calidad principalmente a un grado de traspaso de información en la intranet.

Pazmiño, A. (2011). “Aplicación de hacking ético para la determinación de vulnerabilidades de acceso a redes inalámbricas wifi”. Para establecer vulnerabilidades de accesibilidad a redes inalámbricas wifi a la aplicación de hacking Ético ha sido desplegadoa modo de tesis de investigación, dentro de la Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador, con la finalidad de examinar las técnicas de Hacking y así emplearlasa modo de instrumento de auditoría el cual reporten los peligros que en este tipo de redes se manifiesten y como resultado originar un plan referencial que alcancen los peligros a mitigar y que manifiesten vulnerabilidades de accesibilidad. En esta investigación se ha empleado el método inductivo-deductivo comenzando de una serie secuencial y ordenado de períodos que un hacker sigue y así desarrollar ataques en base de caminos situados en un segmento comercial de la ciudad de Riobamba y asimismo a un router brindado por un ISP, poseyendo al software libre designado BackTrack y Wifiway como distribuciones el cual contribuyana desarrollar dichos ataques y después de dicha estimación se ha desplegado un plan de optimas prácticas y así reducir en redes inalámbricas wifi las probables infracciones no facultadas. Desde una serie de pruebas de penetración en routers inalámbricos se ha desenvuelto los reportes concisos de los procedimientos realizados y en seguida un rango de explotación con su concerniente grado de severidad en un listado de vulnerabilidades categorizadas, al lado con su concerniente peligro y las óptimas prácticas y así conservar la seguridad inalámbrica. De dicho modo se concluyó que en este tipo de redes la seguridad de la información posee una enorme significación concerniente al respaldo de los distintos recursos el cual una entidad o corporación cuenta siendo el activo la información más delicada correspondiendo tener legitimidad, confidencialidad, disponibilidad e integridad, a los usuarios, propietarios de redes inalámbricas, se sugiere, emplear en esta investigación las medidas mostradas y así amortiguar los impactos el cual logren representar la explotación de dichas grietas establecidas, asimismo que debe ser actualizada oportunamente la investigación debido a que son persistentes los incidentes.

Crespo, E. (2013) Tesis Titulada “Hacking ético para pymes" en la Universidad de AZUAY de Ecuador ha brotado en los últimos años la necesidad de salvaguardar la información originada por las compañías ya que ello estima como el activo más significativo actualmente. Al hallarse en su gran parte recopilada y procesada por medios informáticos, para resguardar la información la seguridad se ve orientada en las infraestructuras de tecnología el cual la compañía emplea. Se han venido empleando nuevas metodologías de seguridad para este fin

el cual consienten reconocer vulnerabilidades y con aquello modificar a tiempo los errores, de modo óptimo precautelando la integridad de la indagación. Dicha experiencia es acreditada como hacking ético. Dará una perspectiva clara y puntual esta tesis de que manera se tendrá que desarrollar un proceso de este modelo atravesando por diversos periodos apartir del lado teórico hasta el ámbito práctico aparentando a redes LAN y en páginas webs, ataques a las vulnerabilidades, logrando un manual al finalizar de cómo desarrollar unhacking ético.

2.1.2 Investigaciones nacionales

Aguilar, V. (2015), en su tesis Titulada "Implementación de una solución de hacking ético para mejorar la seguridad en la infraestructura informática de la caja municipal de Sullana - Agencia Chimbote", para optar el Título de ingeniero de sistemas e informática, en laUniversidad Nacional del Santa, Chimbote, Ancash.

Objetivo:

Mejorar la seguridad en la Infraestructura Informática de la Caja Municipal de Sullana - Agencia Chimbote a través de la implementación de una Solución de Hacking Ético. Metodología: Se empleó el método experimental el cual residió en 7 períodos, con la finalidad de desarrollar más precisa y completa una investigación, consintiendo efectuar rectificaciones que requiera en la etapa.

1ra Fase: Estudio bibliográfico sobre Hacking Ético, seguridad informática, Infraestructura Informática y Servicios Financieros.

2da Fase: Recopilación y análisis de la información obtenida de la Caja Municipal de Sullana - Agencia Chimbote.

3ra Fase: Análisis de la Infraestructura Informática de la empresa utilizando la metodología de Hacking.

4ta Fase: Diseño de la Solución de Hacking Ético para la infraestructura informática de la empresa.

5ta Fase: Implementación de la Solución de Hacking Ético para la Infraestructura informática de la empresa.

6ta Fase: Realización de Pruebas a fin de lograr la contratación de la Hipótesis.

7ma Fase: Desarrollo del Informe de Resultados Finales estuvieron formadas los equipos como población por 20 computadoras y 2 servidores, lo conformó la muestra el área de préstamos el cual comprende a 05 computadoras y los 02 servidores alcanzando a conseguir

los siguientes efectos: Los sistemas el cual emplean así como las aplicaciones, operanenorme volumen de carácter confidencial o riesgoso de información de los Clientes, el mismo que debe ser transmitida con la mayor seguridad por medio de la red informática, disminuyendo mínimamente los riesgos informáticos.

Conclusión:

- Se desarrolló la evaluación de la solución propuesta en la Caja Municipal de Sullana consiguiéndose descubrir todas las existentes vulnerabilidades, los mismos que se enmendaron, permaneciendo libre de grietas, lo que da confianza a la gerencia y optimiza la seguridad en el uso de redes de datos y sistemas.
- Se desarrolló la solución a la problemática de la seguridad, se llegó a implementar en la infraestructura informática de la Caja Municipal de Sullana - Agencia Chimbote una solución de hacking ético, con la cual en la transferencia de datos se optimizó la seguridad.

Díaz J., Antonio L. y Salcedo J. (2013) Tesis Titulada: "Sistema de prevención de intrusos para mejorar la seguridad de los servidores de la Universidad Nacional de Trujillo", de la Universidad Nacional De Trujillo, Perú. El temario del reciente trabajo, presentado es Sistema de Prevención de Intrusos para mejorar la seguridad de los servidores de la Universidad Nacional de Trujillo. La oficina de sistemas e informática es el ente encargado de las redes y equipos servidores que mantienen la información de sistemas y datos de la Universidad Nacional de Trujillo. Por tal razón, se describe en el presente trabajo de investigación los movimientos indispensables basados en software libre para la implementación de un sistema de prevención de intrusos, la cual consiente conservar en tiempo real un antecedente e información, referente a probables intentos de accesibilidad o por el lado de usufructuarios no autorizados intentos de vulnerabilidad de los servidores, a través de la alineación de reglamentos el cual se acomoden a los requerimientos auténticosde la agencia de sistemas e informática.

Gonzales C. (2016) Tesis Titulada: "Uso de herramientas de Ethical hacking con kali linux para el diagnóstico de Vulnerabilidades de la Seguridad de la información en la red de la sede central de la Universidad de Huánuco" de la Universidad Nacional de Huánuco, Perú. Ya que hoy por hoy la Información se ha transformado en un ámbito muy significativo del patrimonio-capital, el cual se lograría aseverar que por medio de la información a nivel mundial se mueve todo y a conocimiento de ello es lo que tiene que ofrecer la debida consideración del caso, concerniente a la seguridad caso contrario poseeremos dificultades.

Nos muestran las vulnerabilidades que en un sistema existe debilidad, aquello consentirá a desarrollar a un hacker o cracker un ataque y quebrantar la integridad, confiabilidad, y disponibilidad. Actualmente varios de los sistemas de información de una compañía entre distintas computadoras o subidos a la WEB se encuentran interconectados y entre distintas áreas de trabajo para el desarrollo laboral y la accesibilidad, dichos vínculos en medio de computadoras son distinguidas como REDS LAN.

La razón de la aplicación y ejecución de las herramientas de ethical hacking, son para lograr determinar, evaluar y corregir las vulnerabilidades que en la red de la SEDE central de la universidad de Huánuco existen, y a través de las derivaciones lograremos ofrecer las políticas de seguridad para prevenir dentro de la red y ataques de afuera, del mismo modo enmendar vulnerabilidades existentes.

2.2 Bases teóricas

Arias, F. (1999). Metodología. Fidias G. Arias Odón: asevera que la metodología, para aquello el cual se dedica a indagar, no es una pócima milagrosa al contrario es una sencilla guía a la cual se apela en el momento en que emerge el desconcierto o la incertidumbre, tieneque ver con todo lo vinculado un origen de consulta con los métodos de enseñanza y formas el cual consisten el triunfo del proceso enseñanza-aprendizaje, en la cual dicho tema sería la consecución de los discernimientos indispensables para la instrucción, progreso y entendimiento de distintas formas de aprender una profesión o trabajo en específico. Las metodologías empleadas dentro del transcurso de enseñanza son: la deductiva, la inductiva y la analógica o comparativa.

Una serie de procedimientos, técnicas y soportes documentales utilizados en el bosquejo de sistemas de información. Su finalidad elemental es mostrar un conjunto de técnicas modernas y clásicas de relieve de sistemas el cual consienten desplegar un software de calidad, el cual contienen criterios de comparación de prototipos de sistemas y heurísticas de construcción. Por ende, se define como 3 tipos de metodologías.

Metodología del conocimiento, se encuentra compuesto por un conjunto de componentes el cual consienten la correspondencia en medio del hombre con su medio ambiente. Se encuentran dentro de ella cuatro metodologías universales de conseguir conocimiento:

El método de tenacidad: por medio de dicho procedimiento, deja de creer el individuo en su verdad y arroga como auténtica, la costumbre implantada por un conjunto o asociación de autoridades. El método a priori o de intuición: dicha metodología aprecia que los individuos consiguen obtener llegar a la autenticidad a través del intercambio libre de opiniones y la comunicación; y al no haber un asentimiento entre las partes se ocasiona un dilema al establecer quién tiene el raciocinio.

El método científico: a través de dicha metodología se logran desvanecer todas las inquietudes, que presente el investigador, ya que dicho método, no se fundamenta en opiniones, únicamente se cimienta en derivaciones arrojadas por medio de la experimentación. No admite la autenticidad de una información el científico, si no la somete antes a experimento.

Metodología de la historia, se precisa como un conjunto de procedimientos y técnicas utilizados por los cronistas para maniobrar otras evidencias y las fuentes primarias el cual favorezcan en la averiguación referente a sucesos pasados para las sociedades humanas de enorme significado.

Metodología científica, esta permanece precisada como el procedimiento investigativo empleado esencialmente en la creación de conocimiento fundamentado en las ciencias. **Se designa científico porque se apoya dicha investigación en la medición y en lo empírico**, concordándose a los principios determinados de las pruebas de razón.

Es significativo distinguirse que se encuentran cuatro mecanismos elementales dentro de toda investigación científica: el sujeto (quien la investigación desarrolla); el objeto (el asunto a investigar); el medio (se relata a las técnicas el cual se requieren para desarrollar la investigación); y el fin (corresponde a la finalidad el cual busca la investigación)

Prevención de ataques a los sistemas de información

Operan los cibercriminales de manera clandestina y son dificultosos de descubrir, podría transcurrir bastante tiempo antes de que sean perceptibles las dificultades para la compañía. Toma nota de las siguientes buenas prácticas para la prevención y detección temprana.

- **Evite amenazas a través de emails**

Son uno de los recintos más endebles de una compañía los correos electrónicos, ya que, por medio de ellos, de forma sencilla se pueden introducir peligros de virus y hurto de

información. No obstante, varias compañías creen que no son tan peligrosos y no toman en cuenta la acción de los correos internos y podrían ser víctimas de 'secuestro' de informes. No dejar de lado monitorear los movimientos de mensajes dudosos, tales como las descargas de archivos anexos; instruya a sus colaboradores de su compañía referente al buen empleo de dicho medio con fines laborales para que sea empleado y para que a la compañía alerteen situaciones de ver un correo dudoso.

Detecte a tiempo códigos malicioso

Es frecuente que se oculten estos códigos en archivos PDF, HTML, GIF y Zip. Que no debe dejar de lado una buena práctica, es seleccionar un antivirus idóneo de revelar, decodificar e interpretar estos códigos recónditos y por ende impedir ser víctima de robo de información.

- **Reconozca las conexiones sospechosas**

A menudo los cibercriminales emplean direcciones IP, archivos, sitios web y con un histórico de actividad maliciosa los servidores de correo electrónico. Utilice instrumentos idóneos de inspeccionar la notoriedad de fuentes no confiables situadas en el exterior de su compañía.

Monitoree las bases de datos

La reforma de la estructura dentro del banco de fundamentos y tentativas no acreditados de accesibilidad a información críticos podrían ser señales de alerta el cual señalan que estaría amenazada su red. Utilice instrumentos para registrar tentativas de accesibilidad no acreditado y monitorear bases de datos.

- **Mantenga su sistema actualizado**

El mejor modo de avalar que tengan buen funcionamiento los equipos de la empresa es concibiendo un inventario de todo el hardware utilizable. Luego, elija una técnica para gerenciar de forma más segura sus equipos.

Contamos dos formas de realizarlo: preparar a sus colaboradores para que desarrollen las modernizaciones asiduamente o computarizar el proceso por medio de un instrumento que el sistema actualice mecánicamente. Permitirá esta última opción que de una sola vez se descarguen las actualizaciones y después dentro de la empresa se van distribuyendo.

Hace referencia, metodología del desarrollo de software, en el diseño de sistemas de información, a una serie de sistematizaciones, soportes y procedimientos documentales utilizados. Exponer un conjunto de métodos clásicas y modernas de modelado de sistemas es su principal finalidad el cual consientes desplegar un software de calidad, el cual contienen criterios de comparación de modelos de sistemas y heurísticas de construcción.

Jara, H., & Pacheco, F. G. (2012). Ethical Hacking 2.0. Usershop. Nos muestra para desarrollar el software la metodología, que en lo siguiente reside.

A1:2017-Injection

Dentro de esta categoría se engloban las vulnerabilidades que permiten la inyección de código en herramientas como SQL, NoSQL, OS o LDAP, lo que permite a los servidores interpretar una cadena como si fuese código, pudiendo acceder a la base de datos sinautorización.

A2:2017-Broken Authentication

Fallos en las implementaciones de inicio o gestión de sesión que permite a los atacantes hacerse con contraseñas, claves o cualquier otra información para autenticarse en un sistema temporalmente o de forma permanente.

A3:2017-Sensitive Data Exposure

Debido a fallos en la implementación de distintas APIs, muchas veces no se protege correctamente la información sensible, lo que permite a piratas informáticos hacerse, por ejemplo, con datos personales, bancarios o de salud de usuarios.

A4:2017-XML External Entities (XXE)

Procesadores XLM mal configurados pueden procesar ciertas referencias como si no se tratasen de entradas XML, lo que puede permitir revelar ficheros y recursos ocultos, e incluso ejecutar código o causar un ataque DoS.

A5:2017-Broken Access Control

Errores en la configuración de los sistemas de control de acceso puede permitir a un atacante acceder a recursos y archivos para los que no debería tener permiso.

A6:2017-Security Misconfiguration

Aquí se engloban todo tipo de fallos relacionados con la configuración de todo tipo de sistemas de seguridad, desde las conexiones HTTPS hasta las aplicaciones de seguridad de cualquier sistema o servidor.

A7:2017-Cross-Site Scripting (XSS)

Todo tipo de ataques XSS que se originan cuando una web incluye datos no validados para ejecutar algún script peligroso desde una web que, supuestamente, es de confianza, permitiendo así que la web en cuestión ejecute código en el equipo de la víctima.

A8:2017-Insecure Deserialization

Fallos en la serialización que pueden permitir la ejecución de código directamente en la memoria.

A9:2017-Using Components with Known Vulnerabilities

Como su nombre indica, en esta categoría se recogen todos los usos de librerías, frameworks y otros recursos de software que tienen vulnerabilidades, por lo que, al utilizarlos en una plataforma o un proyecto, automáticamente este se vuelve vulnerable, quedando en peligro a través de estos recursos.

A10:2017-Insufficient Logging & Monitoring

Debido a la falta de monitorización, la mayoría de las veces se tarda hasta 200 días en detectar una vulnerabilidad en un software o una plataforma web, tiempo que se podría reducir notablemente simplemente configurando mayores controles, mejor monitorización y más registros a estas plataformas.

Teoría de Aplicaciones Pentesting y Prevención de Ataques

En todo el mundo las computadoras son susceptibles de ser atacadas por crackers o hackers hábiles de robar información valiosa y comprometer los sistemas informáticos, o bien una gran parte de ella suprimirla. Esta situación hace imprescindible conocer si estos sistemas y redes de datos están protegidos de cualquier tipo de intrusiones. El objetivo de un hacker es explotar las vulnerabilidades red o de un sistema y así hallar la debilidad en uno o más delos dispositivos de seguridad (Confidencialidad, Integridad, Disponibilidad).

Graves, (010) Es un profesional un hacker ético el cual emplea sus destrezas de hacker para propósitos de protección y defensivos, es decir desarrollar experimentos de intrusión y así en la red y los sistemas de seguridad descubrir vulnerabilidades con los mismos instrumentos que un hacker lo haría.

Graves, (2010) Pretende exponer al desarrollar el presente trabajo de investigación referente a las técnicas e instrumentos empleados por los hackers y así descubrir y revelar las vulnerabilidades con el propósito de conocer los mismos instrumentos informáticas con el cual lograríamos ser idóneos de defender nuestra información que para nuestra empresa o institución es un recurso valioso. Usa las habilidades de hacker el hacker malicioso con propósitos maliciosos encaminado en conseguir beneficio económico en gran parte de sus acciones, difundiendo virus fines destructivos, comprometer la operación de los sistemas y las redes, ataque de denegación de servicio. Los motivos que llevan a un hacker a pasarse al lado del mal puede ser por diversión, adquirir conocimientos y experiencia, rivalidad o competencia, ganar reputación, robar, dañar al rival o la competencia perjudicando su imagen en la sociedad y dañando la integridad de la organización revelando información importante, conseguir dinero fácil en obtener información de tarjetas de crédito, poner en

evidencia acciones indebidas de instituciones y personas como es hechos de corrupción, actividad ilícita, hacktivismo entre otros.

2.3 Bases filosóficas

Según Chamorro P. (2016) https://prezi.com/xo8wnlz8v_qs/la-influencia-de-lafilosofia-en- la-tecnologia/ señala que el objetivo de la filosofía de la tecnología es que la filosofía aporta la ideología, es decir la idea general de la naturaleza, donde se circunscribe la tecnología. Un ejemplo: existen ordenadores porque existe la idea de la sociedad de la información. El ordenador es la tecnología y la sociedad de la información es el concepto, es decir la ideología, la filosofía.

Aspectos que aborda la filosofía de la tecnología:

La filosofía, como actividad de crítica y reflexión, aborda la actividad tecnológica y aportaen la elaboración de códigos de ética que posibiliten la correcta utilización del conocimiento en beneficio del hombre.

La filosofía de la tecnología, como nueva disciplina filosófica, permite tener mayor rigurosidad en las definiciones de conceptos y presupuestos en la investigación tecnológica. Dejan abiertas cuestiones la filosofía de la ciencia y la filosofía de la tecnología el cual muestran que para la reflexión filosófica será un campo fructífero y, como contra parte, posibilitan una tecnología más desarrollada la claridad y el alcance filosóficos y, a la vez, moralmente adecuada. Es el conjunto de saberes, conocimientos, habilidades y destrezas interrelacionados con procedimientos para la construcción y uso de artefactos naturales o artificiales que permitan transformar el medio para cubrir necesidades, deseos humanos.

Filósofos que abordaron sobre la tecnología en el siglo XX

Del siglo XX los más significativos filósofos fueron el norteamericano John Dewey y el alemán Martin Heidegger en referirse directamente referente de la tecnología moderna. Sin embargo, ambos consideraron como eje central de la vida moderna a la tecnología, fue optimista Dewey referente al rol de la tecnología, por otro lado, Heidegger fue un poco pesimista. Aquello es una sencilla mención a sus opiniones, no obstante, puede ser visto Heidegger como un crítico, asimismo accesible a la tecnología. La esencia de la tecnología, para Heidegger, es la más grande posibilidad y el más grandioso peligro para la humanidad.

- Llegar a conocer los beneficios y las desventajas de la tecnología en el mundo moderno
- Saber cómo se complementa el hombre de ahora con la tecnología

- Ver el enfoque filosófico de que es la tecnología y para que le sirve esta al hombre actual.

La filosofía de la tecnología del siglo XXI

Según Chamorro P. (2016) en las últimas décadas ha habido un cambio notable en el campo de las tecnologías motivo por cual surgen nuevas disciplinas para encargarse de estudiar esos cambios desde un enfoque filosófico tecnológico, para entender los cambios que se está dando en la sociedad actual en su modo de pensar.

Han reflexionado al transcurrir la historia, científicos y filósofos referentes la ciencia y el conocimiento que ésta nos gestiona. Lo reiterado de ciertos temas como las hipótesis científicas, los papeles respectivos el cual incumben la deducción y a la inducción en la elaboración de la utilidad, la ciencia y la evaluación del progreso y la trascendencia de la matematización del lenguaje científico, a través de las modificaciones (si es que lo hay), es aquello que nos consiente instituir la identidad de una disciplina como Filosofía de la Ciencia. Hacer uso racional de las tecnologías en todos los campos de la vida, teniendo en cuenta las consecuencias que genera para la humanidad y la tierra.

- Hacer uso racional de las tecnologías en todos los campos de la vida, teniendo en cuenta las consecuencias que genera para la humanidad y la tierra.
- La filosofía como ciencia debe preocuparse en un estudio minucioso sobre el progreso de la tecnología que en estos tiempos se está desarrollando y qué debe favorecer a que no pierdan las personas sus principios y valores.
- Todas las disciplinas deben de involucrarse en un trabajo integral para aportar desde su campo y de esa forma entender como las tecnologías influye en la manera de pensar, en su comportamiento de las personas Fundamento filosófico de la tecnología

La Filosofía de la Tecnología

Compone un ambiente de reflexión respectivamente nuevo a la Filosofía de la Tecnología si con otros temas de interés filosófico lo comparamos como la ciencia, la política, el arte.

No obstante conserva tradiciones fortalecidas, en las últimas décadas ha sido cuando ha conseguido atención pública y relevancia académica.

La ética en la seguridad informática

Mendoza M. (2016) de acuerdo este autor conlleva peligros de seguridad el avance de la tecnología vinculados a su empleo, especialmente ya que hay sujetos que sobre los usuarios buscan sacar provecho. Dentro de este argumento, tiene como propósito la mayoría de las amenazas informáticas actualmente formar un beneficio monetario a sus desarrolladores. El cual empezó como curioseo de jóvenes el cual investigan como cambiar el procedimiento de

los sistemas y así maniobraran de una forma en la cual no fueron diseñados, se ha transformado con el paso de los años en una industria de ciberdelitos, atravesando de hackersentusiastas y curiosos a crackers el cual investigan como ganar con sus destrezas. Si se comenten además actos normalizados empleando las recientes tecnologías, suele referirse a ciberdelicuentes.

Por ende, juega un rol predominante la formación profesional dentro del trama de la ciberseguridad, asimismo lo hace la formación personal, el cual posee como fundamento de valores y principios que establecen el proceder los individuos. ¿Qué establece si son buenas o no las acciones de un informático?

La delgada línea entre “el lado del bien y del mal”

El presente paisaje de la ciberseguridad y la seguridad de la información, asimismo como sus propensiones, nos exponen la necesidad de optar por profesionales encomendados de resguardar dentro de cualquier tipo de organización los activos más significativos, así como a sus usufructuarios; sin embargo, se vaticina en el futuro cercano una carencia de personal cualificado. Los conocimientos, habilidades técnicas y aptitudes que ostenten los profesionales de seguridad trascienden elementales para dicha finalidad, no obstante, no debe dejar en segundo plano la formación que considera asimismo el factor humano.

Un individuo que posee los bastantes conocimientos para acceder a información privilegiada y vulnerar un sistema, se hallan delante de una estrecha raya que puede transferir sencillamente y así conseguir un beneficio, al lapso que puede envolver la seguridad de usuarios y compañías. Únicamente le permite discernir su formación ética en ciberseguridad en medio de lo que podría ser estimado como malo o bueno, y por supuesto, lo que es reglamentario o no.

Acordemos la cuestión de Edward Snowden, él era un usuario permitido para ingresar a una enorme cantidad de sistemas privados, y ningún organismo es capaz conservar la confiabilidad si decide violarla un usuario en el que confía, indicaba el investigador de ESETStephen Cobb. Pero incluso se deben considerar otros aspectos, como la personalidad misma. Esta responde a un sin número de estímulos, tanto internos como externos, donde pueden incluirse los intereses, ideologías, motivaciones, experiencias, la formación desde el hogar o la escuela. Por lo tanto, la personalidad se determina a través del carácter (innato) y el temperamento (experiencias y educación) que también es fundamental en el ejercicio profesional. En el ámbito corporativo, a la hora de elegir profesionales, puede haber personas bienintencionadas y otras no tanto, por lo que a veces la elección se limita a conocer lo mejor

posible la voluntad y las intenciones de la persona, y si está realmente interesada en el hacking ético o tendrá siempre un costado que genera dudas. Muchos de los que hoy son expertos en seguridad han experimentado con el hacking en su juventud y primeros años en el mundo informático, pero en cada caso hay matices que separan, por ejemplo, a quien usó una vez un gusano simple para molestar a sus amigos, de quien desarrolló un malware destructivo, administró una botnet, robó información personal o confidencial o lucró a costa de engañar a otros usuarios. Este es un debate de nunca acabar en esta industria. Por lo tanto, una tarea en la que se debe trabajar es en la formación de profesionales de seguridad con las habilidades técnicas necesarias para la protección, pero al mismo tiempo con sentido de responsabilidad y ética para el ejercicio de sus actividades.

Moral, ética, leyes y su propósito principal

Una condición ideal, en un ámbito de mayor amplitud, consistiría en la coherencia y alineación en medio de la ética, la moral y las leyes que proceden de las diversas naciones; no obstante, esto no es viable en momentos. También, varían estos elementos de una sociedad a otra, y con el tiempo se modifican. El propósito elemental que dentro del contextode los encargados de la ciberseguridad y la seguridad de la información se debería apremiares sin afectar a otro, proceder y tomar determinaciones. Ello establecería una conducta éticay profesional, sin duda una labor aplazada y que representa con implicaciones un enorme esfuerzo no solo laboral sino también social.

2.4 Definición de términos básicos

Algoritmo

Se denomina algoritmo a un grupo finito de operaciones organizadas de manera lógica y ordenada que permite solucionar un determinado problema. Se trata de una serie de instrucciones o reglas establecidas que, por medio de una sucesión de pasos, permiten arribar a un resultado o solución.

Local File Inclusion

Esta técnica consiste en incluir ficheros locales, es decir, archivos que se encuentran en el mismo servidor de la web con este tipo de fallo - a diferencia de Remote File Inclusión o inclusión de archivos remotos (RFI) que incluye archivos alojados en otros servidores.

Intruso

Es aquel que, sin derecho a ello, ocupa un cargo o está en un lugar que no le corresponde.De ahí se deriva la sinonimia con voces que ponen el acento en la situación de ser ajeno que presenta una cosa o una persona.

Hacker

De forma errónea se ha catalogado a los hackers como una sola comunidad, sin embargo, existe una clasificación dentro de ellos que separa las intenciones de cada uno. Veamos en seguida dichas clasificaciones que nos servirán para entender sus propósitos. White Hacker Los White Hat Hackers también ejercen el control a la hora de vulnerar sistemas, sinembargo, ellos lo hacen para estudiar y fortalecer los fallos encontrados. Se dice que algunosWhite Hat Hackers pertenecieron al bando de los Black Hat Hackers y hoy utilizan todos sus conocimientos para mejorar los sistemas en materia de seguridad.

Grey Hacker

Este es el tipo de Hackers que usan sus habilidades para traspasar los niveles de seguridad y luego ofrecen sus servicios como administradores de seguridad informática para corregir dichos errores. De esta forma atacando diferentes servicios demuestran sus conocimientos para luego ofrecer defenderlos.

Black Hacker

Conocidos como sombreros negros son aquellos que realizan actividades para vulnerar la seguridad de sistemas, violentar y extraer información restringida con un fin monetario. Entre otras actividades también son creadores de virus, spywares y malwares.

Pentest

Pentesting o Penetration Testing es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas.

Black Box Testing

Pruebas de caja negra y pruebas funcionales. En los estándares para Software Testing definidos por ISTQB, las técnicas de pruebas de caja negra son utilizadas para realizar pruebas funcionales, basadas en las funciones o características del sistema y su interacción con otros sistemas o componentes

Firewall

Un firewall actúa como defensa contra virus, gusanos, troyanos y ataques de fuerza bruta. Puede adoptar la forma de software (un programa de seguridad) o de hardware (router físico), pero en ambos casos realiza la misma función: analiza el tráfico de red entrante para asegurarse de que no contenga datos incluidos en la lista negra. Los firewalls analizan cada "paquete" de datos (fragmentos pequeños de un gran conjunto, de tamaño reducido para facilitar su transmisión) a fin de garantizar que estos paquetes no contengan ningún elemento malicioso.

Prueba de intrusión de aplicación web

Una prueba de intrusión o intrusión es un método de evaluación de la seguridad de un sistema de ordenadores o una red a través de un simulacro de un ataque. Una prueba de intrusiones de aplicación web está enfocada solamente a aprecia la seguridad de una aplicación web. El proceso conlleva un análisis activo de la aplicación en busca de cualquier debilidad, fallos técnicos o vulnerabilidades. Cualquier incidencia de seguridad que sea encontrada será presentada al propietario del sistema, junto con una evaluación de su impacto, y a menudo con una propuesta para su mitigación o una solución técnica.

2.5 Hipótesis de investigación

2.5.1 Hipótesis general

Existe una relación directa y significativa entre la Aplicación de Pentesting y la prevención de ataques a los sistemas de Industrias San Miguel del Sur – Planta Huaura 2019.

2.5.2 Hipótesis específicas

- Existe una relación directa y significativa entre la configuración y la prevención de ataques a los a los sistemas de Industrias San Miguel del Sur – Planta Huaura 2019.

- Existe una relación directa y significativa entre la caja negra y la prevención de ataques a los sistemas de Industrias San Miguel del Sur – Planta Huaura 2019.

- Existe una relación directa y significativa entre la criptografía y la prevención de ataques a los sistemas de Industrias San Miguel del Sur – Planta Huaura 2019.

2.6 Operacionalización de las variables

Variables	Conceptualización	Dimensiones	Indicadores
Variable I Aplicación de Pentesting	El Pentesting es una acción constituida por un conjunto de "test de penetración", o penetration tests, que se basan en ataques hacia los sistemas informáticos con la intención de encontrar sus debilidades o vulnerabilidades	**1.1 Configuración**	- Motor de base de datos - Puertos Abiertos - Contraseña Débil
		1.2 Caja Negra	- Inyección SQL - Validación de Datos - Inclusión de Archivos
		1.3 Criptografía	- Algoritmo
Variable II Prevención de ataques a los sistemas de industrias San Miguel del sur-Planta Huaura	Es el Monitorios de intentos no autorizados de acceso a datos críticos y de modificación de la estructura en las bases de datos son señales de alerta que indican que su red puede estar siendo amenazada	**2.1. Actualización**	- Versiones
		2.2. Preventor	- Firewall - IDS - WAF
		2.3 Administración de Privilegios	- Rol de Usuario

CAPÍTULO III
METODOLOGÍA

3.1 Diseño metodológico

3.1.1. Tipo

La presente investigación tiene como tipo de diseño la investigación no experimental, descriptiva y Correlacional. Hernández, Fernández & Baptista (2014) señalan que las investigaciones de diseño no experimental se definen como las investigaciones que se realizan sin manipular deliberadamente a las variables de estudio. Esto significa que se refiere de estudios en la cual no se hace variar a las variables independientes de forma intencional para ver su influencia referente a otras variables.

El Tipo de investigación es aplicativa, porque se trata solo de conocer la correlación entre las variables I Aplicación de Pentesting y II Prevención de Ataques, posteriormente con una investigación aplicada será con el propósito de brindar una práctica solución de los ataques a los sistemas de Industrias San Miguel del Sur – Planta Huaura, de esta manera mejorar la seguridad de los sistemas de informática de dicha industria.

3.1.2. Nivel

La presente investigación corresponde al nivel correlacional.

3.1.3. Método

En el presente estudio se utilizó principalmente el método deductivo, porque se parte de los conocimientos generales ya existentes para aplicar dichos conocimientos a casos particulares en este caso en las empresas de cuerdo sus necesidades en el campo de los sistemas informáticos. Así mismo el método deductivo consiste en la totalidad de reglas y procesos, con cuya ayuda es posible deducir conclusiones finales a partir de enunciados supuestos llamados premisas.

3.2 Población y muestra

3.2.1 Población

La población estuvo conformada por 30 trabajadores de la Oficina de Informática de Industrias San Miguel del Sur.

3.2.2 Muestra

Por su parte Hernández citado en Castro (2003), manifiesta que "si la población es menor a cincuenta (50) individuos, la población es igual a la muestra" (p.69), por lo tanto, la muestra será de 30 trabajadores.

En la presente investigación se aplicó el muestreo por conveniencia del investigador, ya que es una técnica de muestreo no probabilístico y no aleatorio utilizada para crear muestras de acuerdo a la facilidad de acceso, la disponibilidad de las personas de formar parte de la muestra, en un intervalo de tiempo dado o cualquier otra especificación práctica de un elemento particular.

3.3 Técnicas de recolección de datos

Se empleó en la presente investigación la técnica de la encuesta, cuyo instrumento demedición utilizado fue el cuestionario tipo escala Likert, el más usual en un trabajo de investigación científica de nivel correlacional.

La Escala Aplicación de Pentesting, cuya estructura está conformada por 12 ítems y medirá 3 dimensiones: Configuración, Pruebas de caja negra y Criptografía.

Administración; la escala de Likert se aplicó en forma individual a los 30 trabajadores dela Oficina de Informática de Industrias San Miguel del Sur- Planta Huaura.

Tiempo de aplicación; fue aproximadamente de 20 minutos

Calificación y puntuación; la calificación fue manual y la puntuación oscila entre 60 (puntuación mayor) y 12 (puntuación menor).

La gradiente; es la siguiente:

1 = Totalmente en Desacuerdo

2 = En Desacuerdo

3 = Ni de Acuerdo ni en Desacuerdo

4 = De acuerdo

5 = Totalmente de acuerdo.

La confiabilidad del instrumento de medición será a través del Alfa de Cronbach.

La Escala Prevención de Ataques a los Sistemas de Industrias San Miguel del Sur-Planta Huarua. cuya **estructura** está conformada por 20 ítems y medirá 3 dimensiones: Actualización, Preventor y Administración de privilegios.

Administración; la escala se aplicó en forma individual a los 30 trabajadores de la Oficina de Informática de Industrias San Miguel del Sur-Planta Huaura.

Tiempo de aplicación; fue aproximadamente de 20 minutos

Calificación y puntuación; la calificación fue manual y la puntuación oscila entre 100 (puntuación mayor) y 20 (puntuación menor).

La gradiente; es la siguiente:

1 = Totalmente en Desacuerdo

2 = En Desacuerdo

3 = Ni de Acuerdo ni en Desacuerdo

4 = De acuerdo

5 = Totalmente de Acuerdo.

La confiabilidad será medida a través del Alfa de Cronbach

3.4 Técnicas para el procesamiento de la información

Para el procesamiento y análisis de datos se utilizó el software Statical Package for the Social Sciences - SPSS versión N° 23 A nivel descriptivo los resultados se presentarán mediante el análisis de datos en el primer momento se analizará a través de medidas de tendencia central, media y desviación estándar obtenidas tanto en la variable Aplicación de Pentesting, como en la variable Prevención de ataques, en relación de percepción de los trabajadores de la Oficina de Informática de Industrias San Miguel del Sur-Planta Huaura. En el segundo momento se analizó e interpretó los datos a través de tablas y figuras descriptivas.

A nivel inferencial se contrastaron las hipótesis tanto general y específicos utilizando el Coeficiente de Correlación de Pearson, interpretando el grado de correlación de las variables con la finalidad de elaborar las conclusiones y recomendaciones de la presente investigación.

CAPÍTULO IV

RESULTADOS

4.1 Análisis de resultados

4.1.1 Propuesta de la aplicación de Pentesting

4.1.1 Propuesta de red privada virtual (VPN)

Figura 1. Propuesta red VPN Industrias San miguel del Sur-Planta Huaura

4.1.2 Aplicación de Pentesting a los sistemas de industrial san miguel planta Huaura

4.1.2.1 Estatus del cierre de periodos 2018 sistema contable de industrias san miguel del sur planta Huaura

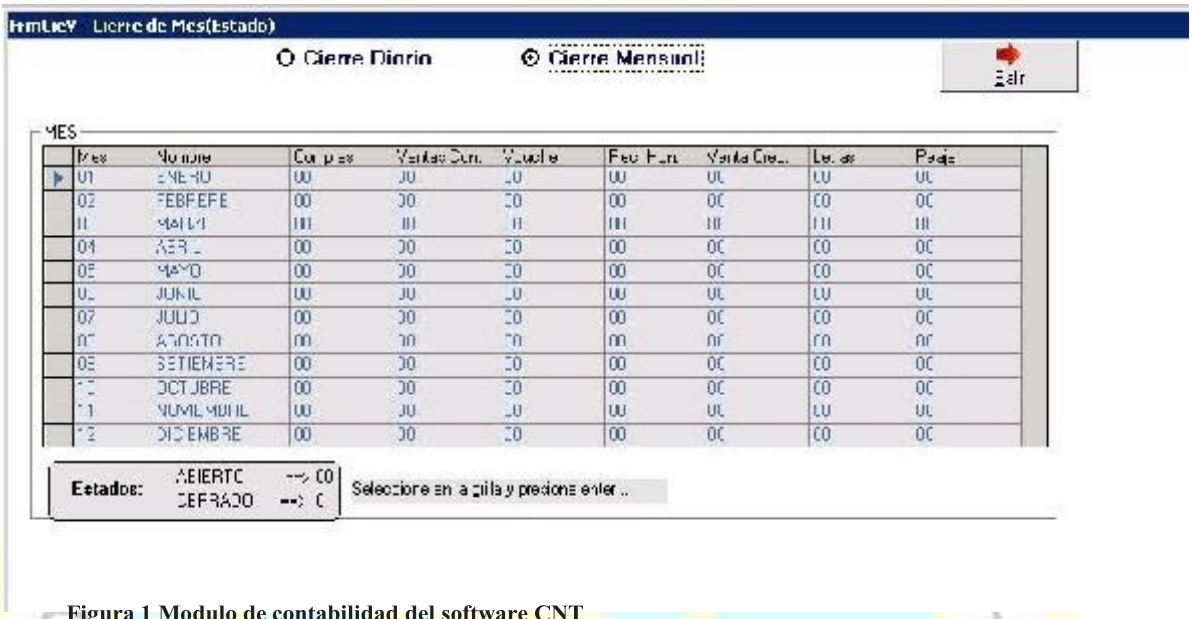


Figura 1 Modulo de contabilidad del software CNT

Tabla 1

Evidencia de vulnerabilidades del software CNT

Análisis evidencias	Levantamiento observación
F. Vulnerabilidad de accesos al sistema Identificamos una "Back door" (puerta trasera) que permite el control de la base de datos; se realizó la Aplicación de Ingeniería Inversa para la obtención del algoritmo de desencriptación de la cadena de conexión a la base de datos (IP o nombre del servidor, **usuario y contraseña).** **Esta vulnerabilidad involucra los sistemas de Brhusa y Agro ISM, generando el riesgo latente de pérdida de información y/o fraudes informáticos (manipulación de cuentas bancarias en planillas, AFP, entre otros)** .	Al área de sistemas, eliminar los siguientes archivos: - ProyEncrypta.exe - Seguridad.exe - Encripta.exe A la GAF, proyectar en mediano plazo una reestructuración del sistema, para reducir los riesgos indicados.

4.1.2.2 Revisión del sistema análisis pentesting usando ingeniería inversa

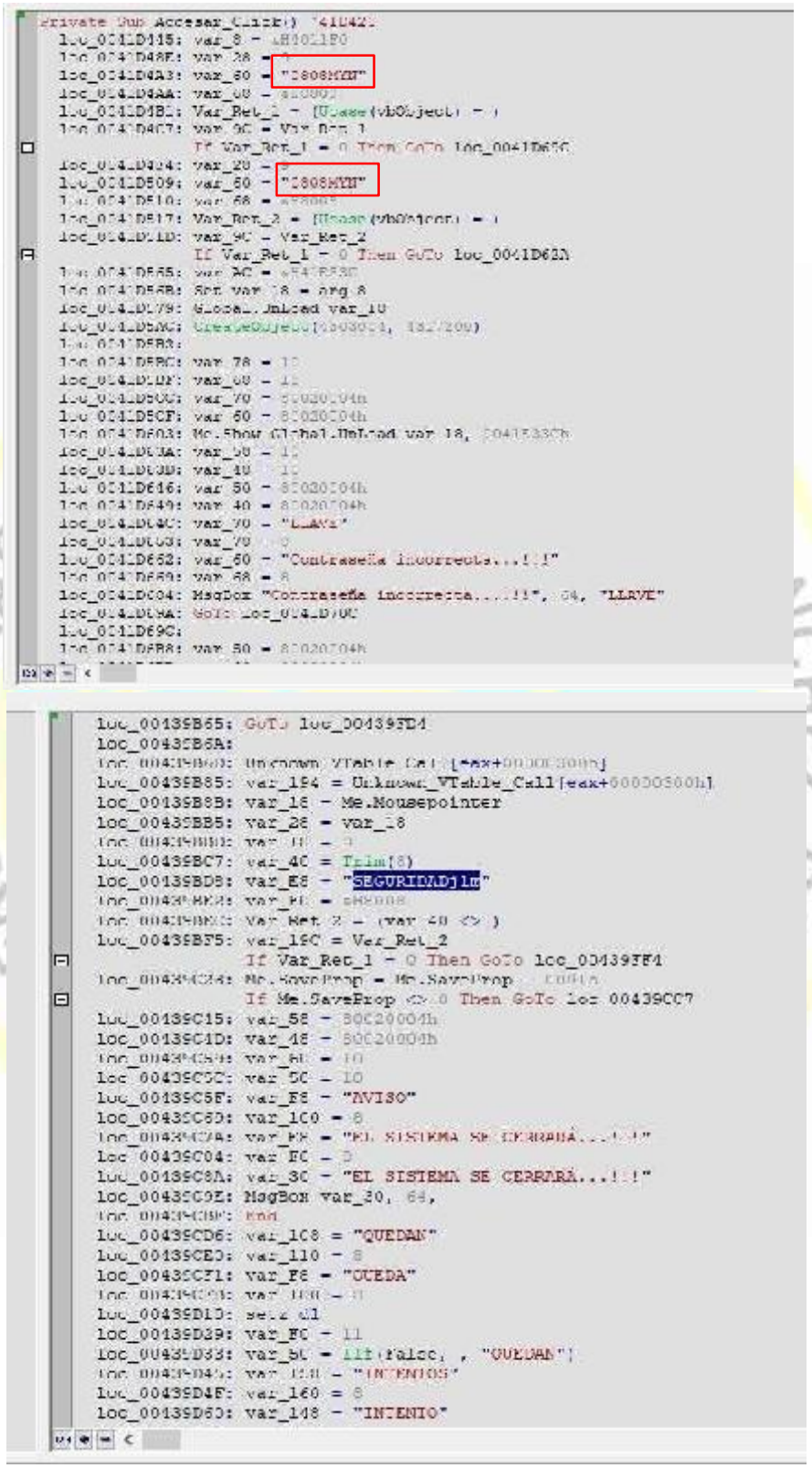


Figura 2. Aplicación de ingeniería inversa obtener sistema contable

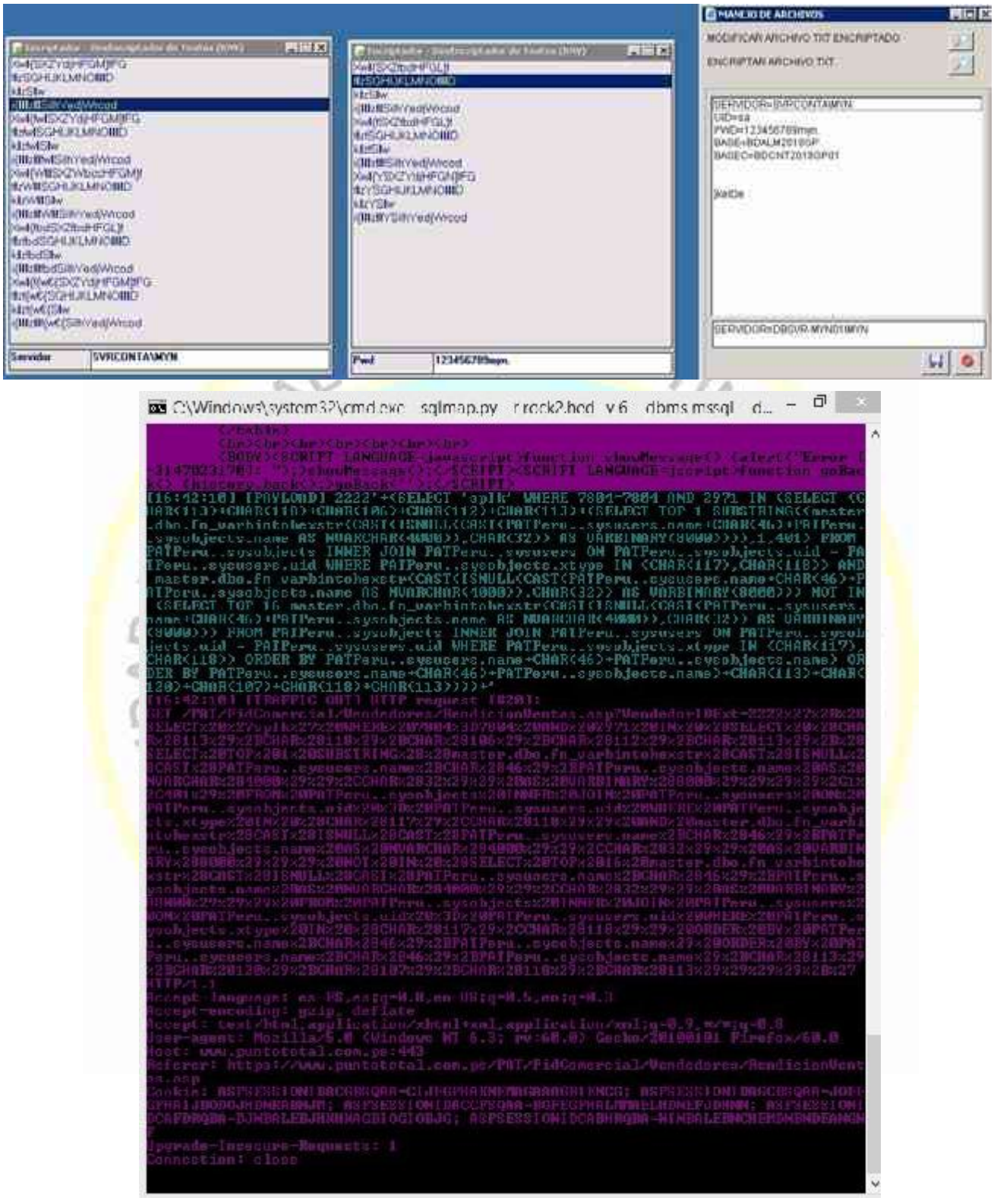
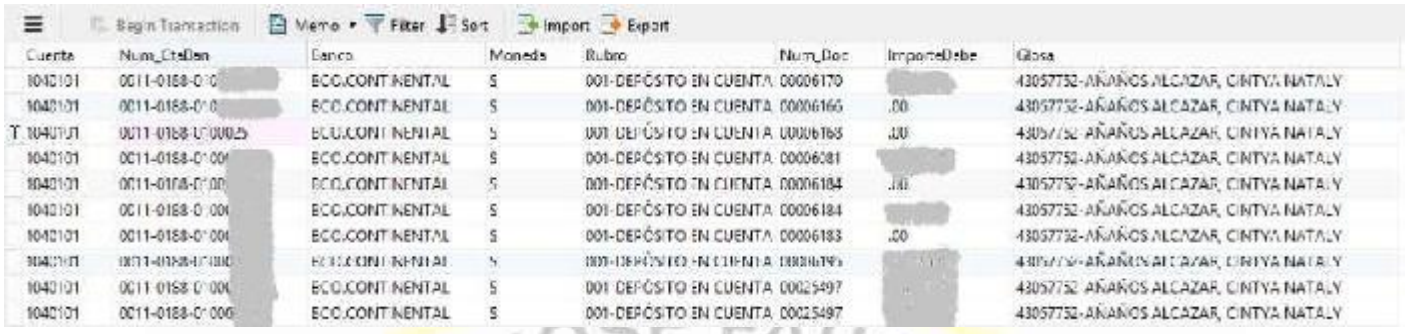
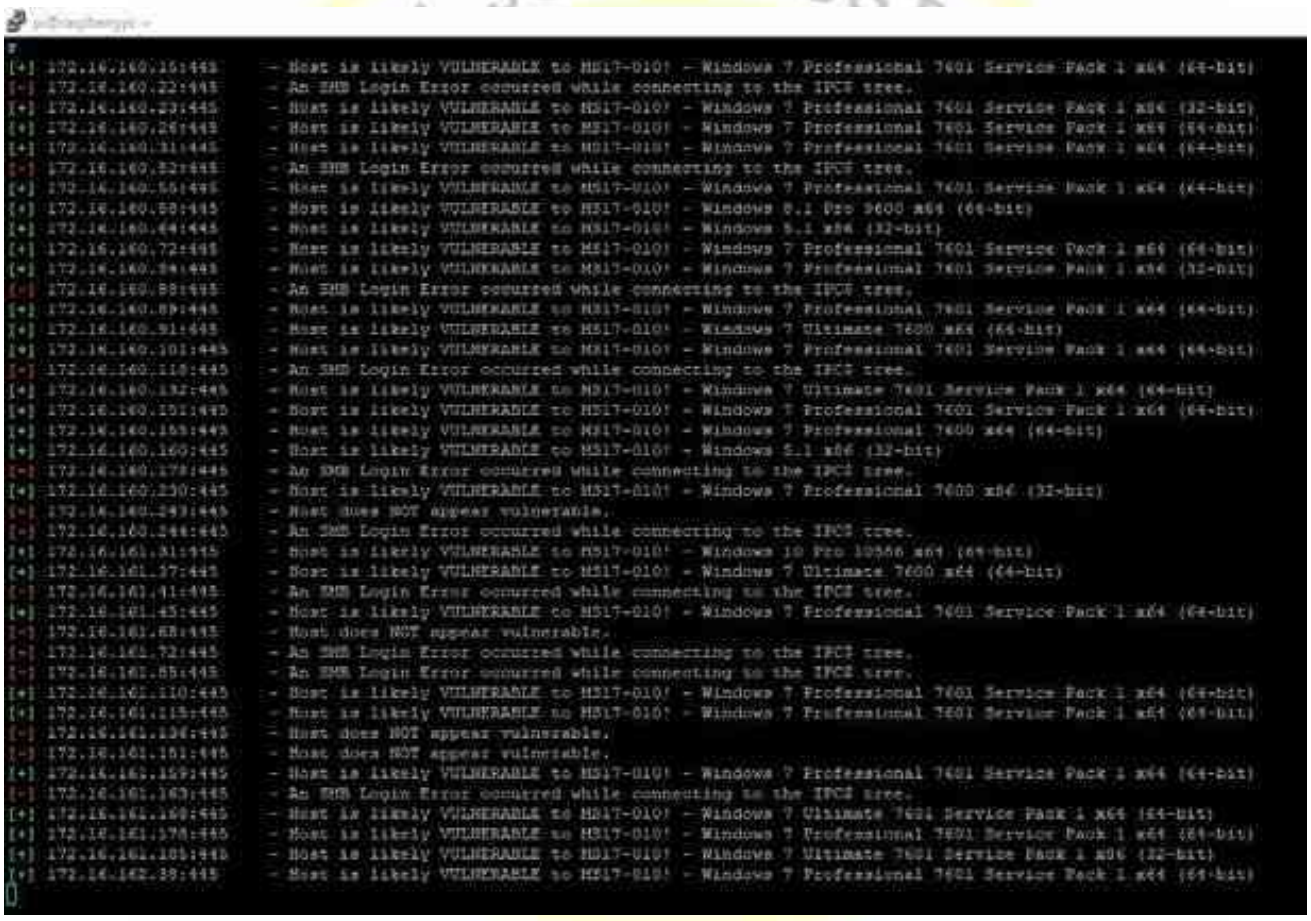


Figura 3 Obtención del Password a través de ingeniería inversa - evidencia



Begin Transaction | Menu | Filter | Sort | Import | Export

Cuenta	Num_CtaBan	Banco	Moneda	Rubro	Num_Doc	ImporteDebe	Glosa
1042101	0011-0168-0[redacted]	BCO.CONTINENTAL	S	001-DEPÓSITO EN CUENTA	00006170	[redacted]	43057752-AÑAÑOS ALCAZAR, CINTYA NATALY
1042101	0011-0168-0[redacted]	BCO.CONTINENTAL	S	001-DEPÓSITO EN CUENTA	00006166	.00	43057752-AÑAÑOS ALCAZAR, CINTYA NATALY
1042101	0011-0168-0[redacted]	BCO.CONTINENTAL	S	001-DEPÓSITO EN CUENTA	00006168	.00	43057752-AÑAÑOS ALCAZAR, CINTYA NATALY
1042101	0011-0168-0[redacted]	BCO.CONTINENTAL	S	001-DEPÓSITO EN CUENTA	00006181	[redacted]	43057752-AÑAÑOS ALCAZAR, CINTYA NATALY
1042101	0011-0168-0[redacted]	BCO.CONTINENTAL	S	001-DEPÓSITO EN CUENTA	00006184	.00	43057752-AÑAÑOS ALCAZAR, CINTYA NATALY
1042101	0011-0168-0[redacted]	BCO.CONTINENTAL	S	001-DEPÓSITO EN CUENTA	00006184	[redacted]	43057752-AÑAÑOS ALCAZAR, CINTYA NATALY
1042101	0011-0168-0[redacted]	BCO.CONTINENTAL	S	001-DEPÓSITO EN CUENTA	00006183	.00	43057752-AÑAÑOS ALCAZAR, CINTYA NATALY
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1042101	0011-0168-0[redacted]	BCO.CONTINENTAL	S	001-DEPÓSITO EN CUENTA	00025497	[redacted]	43057752-AÑAÑOS ALCAZAR, CINTYA NATALY
1042101	0011-0168-0[redacted]	BCO.CONTINENTAL	S	001-DEPÓSITO EN CUENTA	00025497	[redacted]	43057752-AÑAÑOS ALCAZAR, CINTYA NATALY



```
[+] 172.16.160.161:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[-] 172.16.160.22:445     - An SMB Login Error occurred while connecting to the IPC$ tree.
[+] 172.16.160.23:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x86 (32-bit)
[+] 172.16.160.26:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[+] 172.16.160.31:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[-] 172.16.160.32:445     - An SMB Login Error occurred while connecting to the IPC$ tree.
[+] 172.16.160.55:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[+] 172.16.160.58:445     - Host is likely VULNERABLE to MS17-010! - Windows 8.1 Pro 9600 x64 (64-bit)
[+] 172.16.160.64:445     - Host is likely VULNERABLE to MS17-010! - Windows 8.1 x86 (32-bit)
[+] 172.16.160.72:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[+] 172.16.160.84:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x86 (32-bit)
[-] 172.16.160.88:445     - An SMB Login Error occurred while connecting to the IPC$ tree.
[+] 172.16.160.89:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[+] 172.16.160.91:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7600 x64 (64-bit)
[+] 172.16.160.101:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[-] 172.16.160.110:445    - An SMB Login Error occurred while connecting to the IPC$ tree.
[+] 172.16.160.132:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[+] 172.16.160.151:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[+] 172.16.160.153:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64 (64-bit)
[+] 172.16.160.160:445    - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[-] 172.16.160.178:445    - An SMB Login Error occurred while connecting to the IPC$ tree.
[+] 172.16.160.230:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x86 (32-bit)
[-] 172.16.160.243:445    - Host does NOT appear vulnerable.
[-] 172.16.160.244:445    - An SMB Login Error occurred while connecting to the IPC$ tree.
[+] 172.16.161.31:445     - Host is likely VULNERABLE to MS17-010! - Windows 10 Pro 10586 x64 (64-bit)
[+] 172.16.161.37:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7600 x64 (64-bit)
[-] 172.16.161.41:445     - An SMB Login Error occurred while connecting to the IPC$ tree.
[+] 172.16.161.45:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[-] 172.16.161.68:445     - Host does NOT appear vulnerable.
[-] 172.16.161.72:445     - An SMB Login Error occurred while connecting to the IPC$ tree.
[-] 172.16.161.85:445     - An SMB Login Error occurred while connecting to the IPC$ tree.
[+] 172.16.161.110:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[+] 172.16.161.115:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[-] 172.16.161.136:445    - Host does NOT appear vulnerable.
[-] 172.16.161.161:445    - Host does NOT appear vulnerable.
[+] 172.16.161.169:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[-] 172.16.161.183:445    - An SMB Login Error occurred while connecting to the IPC$ tree.
[+] 172.16.161.160:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[+] 172.16.161.178:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[+] 172.16.161.185:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x86 (32-bit)
[+] 172.16.162.39:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
```

Figura 4. Evidencia de vulnerabilidad, para visualización y posibilidad de edición de información confidencial, base de datos (bancos Brhusa).

4.2 Contrastación de hipótesis

4.2.1 Validación de instrumento

La validez del instrumento (Instrumento para la toma de datos) de la presente investigación, se realizó por medio del juicio de expertos, en donde ellos evaluaron y a criterio propio calificaron el contenido del cuestionario empleado. Los expertos el cual desarrollaron la validación fueron los siguientes:

El primer instrumento que se seleccionó corresponde a la variable: **Aplicación de Pentesting** y el segundo instrumento: **Sistemas** La validación de los instrumentos se realizó con los docentes expertos en investigación de la Universidad Nacional José Faustino Sánchez Carrión. Se elaboró los instrumentos de investigación, los cuales contiene 15 ítems. La validación de los instrumentos de recolección de datos se realizóa través de los siguientes procedimientos: Validez de contenido.

Sabino, Carlos (1992, pág. 154), concernientes a la Validez, sostiene: “Para que una escala pueda considerarse como capaz de aportar información objetiva debe reunir los siguientes requisitos básicos: validez y confiabilidad”.

De lo expuesto en el párrafo anterior, se define la validación de los instrumentos como la determinación de la capacidad de las encuestas para medir las cualidades para lo cual fueron construidos.

Se les entregó a los referidos expertos la matriz de consistencia, los instrumentos y la ficha de validación en la cual se establecieron: referente a la base del procedimiento de validación descrita, consideraron los expertos que la existencia de una estrecha relación es pertinente en medio de los criterios y objetivos del estudio y los ítems constitutivos de los dos instrumentos de recopilación de la información.

Se presenta a continuación la cuantificación de las calificaciones de los expertos en la siguiente tabla:

Tabla 2

Nivel de validez de las encuestas, según el juicio de expertos

EXPERTOS	%
Mg. Chávez Zabaleta, Raúl	84
Mg. Palomino Tiznado Máximo	85
Mg. Martínez Infante, Pedro	83
Mg. Pérez Ramírez, José	84
PROMEDIO DE VALORACIÓN	84

Los valores resultantes, después de tabular la calificación emitida por los expertos, están considerados a un nivel de validez muy bueno.

Los resultados pueden ser comprendidos mediante el siguiente cuadro que presentamos en la tabla

Tabla 3

Valores de los niveles de validez

VALORES	NIVELES DE VALIDEZ
91 – 100	Excelente
81 – 90	Muy bueno
71 – 80	Bueno
61 – 70	Regular
51 – 60	Deficiente

El cálculo del Coeficiente de Validez del instrumento se realizó usando el método Delphi. La matriz de análisis de Juicio de Expertos se encuentra en el anexo Nº 1.

El coeficiente de Validez del instrumento es de 84%, es considerado como Excelente validez

Con una validez general de 84% según la escala de validez el instrumento tiene Excelente validez; aplicación de Pentesting y prevención de ataques a los sistemas de industrias san miguel del sur, de acuerdo al criterio de los expertos. Ver tabla No 3.

4.2.2 Confiabilidad

Se ejecutó el análisis de fiabilidad en el programa estadísticos SPSS Statistics 23.0 al instrumento aplicado a todos los integrantes de la unidad de industrias san miguel del sur (jefes del Área, Personal técnico,).

Se adquirió una fiabilidad por variable (ver tabla 4), estuvo conformado por 15 ítems, distribuidos para la **variable I:** *Aplicación de Pentesting* y para la **variable II:** *prevención de ataques a los sistemas de industrias San Miguel del Sur*.

Este quiere decir que el instrumento tiene una valoración de alta validez según la escala de expertos.

La confiablidad del Cuestionario se desarrolla con los mismos resultados de la utilización piloto para su evaluación se utiliza el coeficiente alfa de Cronbach, cuya expresión es:

El coeficiente alfa de Cronbach del test, calculado con el SPSS 23 es 0, 886 y la segunda variable respectivamente 0.853, con el cual finaliza que el cuestionario es confiable.

Tabla 4

Resultados de Confiabilidad por variable

Variable: APLICACION DE PENTESTING

ESTADÍSTICOS DE FIABILIDAD	
Alfa de Cronbach	N de elementos
,886	15

Tabla 5 ***Resultado de Confiabilidad de la segunda variable***

Variable: PREVENCIÓN DE ATAQUE A LOS SISTEMAS INDUSTRIAS SAN MIGUEL DEL SUR

ESTADÍSTICOS DE FIABILIDAD	
Alfa de Cronbach	N de elementos
,853	15

En consecuencia, el instrumento de investigación es plenamente aceptable y aplicable, según la tabla de valoración siguiente:

Tabla 6

Valores de los niveles de confiabilidad

VALORES	NIVEL DE CONFIABILIDAD
0,53 a menos	Confiabilidad nula
0,54 a 0,59	Confiabilidad baja
0,60 a 0,65	Confiable
0,66 a 0,71	Muy confiable
0,72 a 0,99	Excelente confiabilidad
1,0	Confiabilidad perfecta

Dado que la aplicación del instrumento a una muestra piloto es significativa, podemos afirmar que el instrumento es confiable y, por lo tanto, aplicable a diferentes instituciones del mismo nivel educativo y los resultados que se obtengan también serán similares.

4.2.3 Presentación de cuadros e interpretación

En este capítulo se estudian los resultados obtenidos por medio del instrumento.

Es elemental en este capítulo, los datos contribuidos por los trabajadores de la Oficina de Informática del Industrias San miguel del Sur-Planta Huaura, en la cual la información sirvió para conseguir conclusiones y recomendaciones.

A. Datos Generales

Como se ha señalado el número total de encuestados es de 30 personas que trabajan en la Oficina de Informática del Industrias San miguel del Sur.

A continuación, se mostrará las tablas de esta distribución.

ITEM 1: ¿El Conocimiento que tiene respecto a la vulnerabilidad de los sistemas, permite detectarlos con facilidad en el Industrias San miguel del Sur – Planta Huaura ?

Tabla 7

El Conocimiento que tiene respecto a la vulnerabilidad de los sistemas, permite detectarlos con facilidad en el Industrias San miguel del Sur

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Desacuerdo	3	10,0	10,0	10,0
	Ni acuerdo	6	20,0	20,0	30,0
	De acuerdo	21	70,0	70,0	100,0
	Total	30	100,0	100,0	

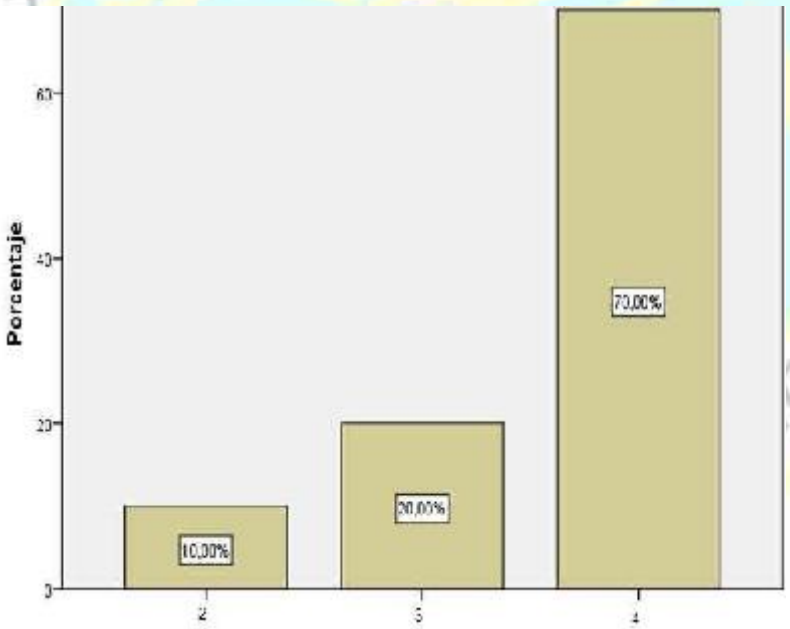


Figura 5 El Conocimiento que tiene respecto a la vulnerabilidad de los sistemas, permite detectarlos con facilidad en el Industrias San Miguel del Sur Planta- Huaura

En la Tabla 7 y Figura 5, que corresponde al ítem 1, se puede observar que del 100% (30) de trabajadores encuestados, el 70% refieren como algo De acuerdo, y el 20 % no están de acuerdo. Por lo tanto, se desprende que el 10% está en desacuerdo.

ITEM 2: ¿El Motor de base de datos de la Aplicación de Pentesting aplicado, previene la vulnerabilidad del Sistemas del Industrias San Miguel – Planta Huaura?

Tabla 8

El Motor de base de datos de la Aplicación de Pentesting aplicado, previene la vulnerabilidad del Sistemas del Industrias San miguel del sur planta Huaura

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Total desacuerdo	3	10,0	10,0	10,0
	Desacuerdo	3	10,0	10,0	20,0
	Ni acuerdo	15	50,0	50,0	70,0
	De acuerdo	9	30,0	30,0	100,0
	Total	30	100,0	100,0	

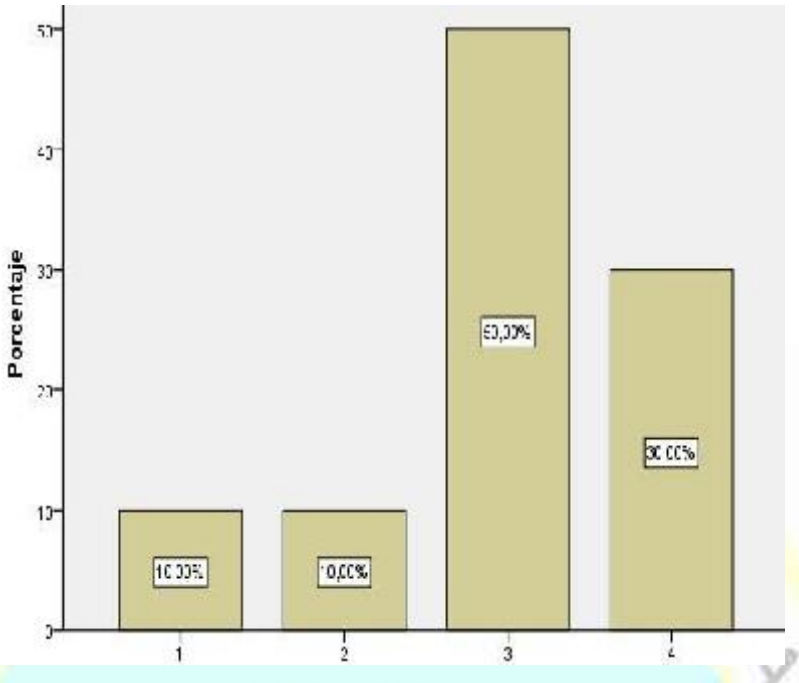


Figura 6. El Motor de base de datos de la Aplicación de Pentesting aplicado, previene la vulnerabilidad del Sistemas del Industrias San miguel del sur planta Huaura

En la Tabla 8 y Figura 6, que corresponde al ítem 2, se puede observar que del 100% (30) de trabajadores encuestados, el 50% refieren como algo Ni de acuerdo, y el 30 % están de acuerdo. Por lo tanto, se desprende que el 10% está en desacuerdo y total desacuerdo.

ITEM 3: ¿La Implementación del procedimiento almacenado y triggers en el Motor de base de datos detecta la intrusión en el sistema web del Industrias San Miguel del Sur Planta-Huaura ?

Tabla 9

La Implementación del procedimiento almacenado y triggers en el Motor de base de datos detecta la intrusión en el sistema del Industrias San miguel del Sur.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Desacuerdo	9	30,0	30,0	30,0
	No de acuerdo	6	20,0	20,0	50,0
	De acuerdo	15	50,0	50,0	100,0
	Total	30	100,0	100,0	

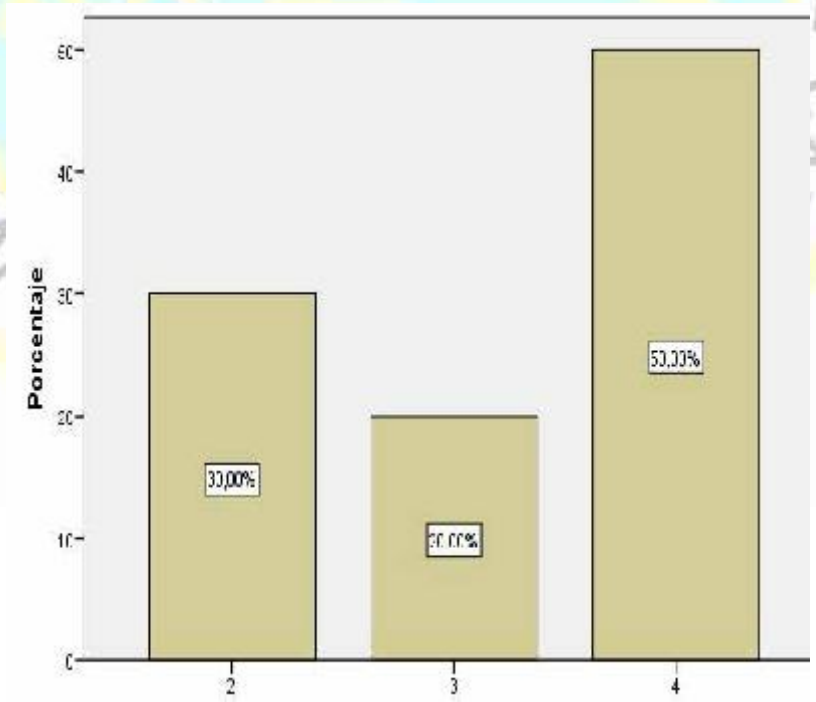


Figura 7. La Implementación del procedimiento almacenado y triggers en el Motor de base de datos detecta la intrusión en el sistema del Industrias San miguel del Sur.

En la Tabla 9 y Figura 7, que corresponde al ítem 3, se puede observar que del 100% (30) de trabajadores encuestados, el 50% refieren como algo De acuerdo, y el 30 % están en desacuerdo. Por lo tanto, se desprende que el 20% No están de acuerdo.

ITEM 4: ¿La adecuada configuración de los puertos abiertos, aumenta nivel de vulnerabilidad de los sistemas?

Tabla 10

La adecuada configuración de los puertos abiertos, aumenta el nivel de vulnerabilidad de los sistemas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Total desacuerdo	9	30,0	30,0	30,0
	Desacuerdo	15	50,0	50,0	80,0
	De acuerdo	6	20,0	20,0	100,0
	Total	30	100,0	100,0	

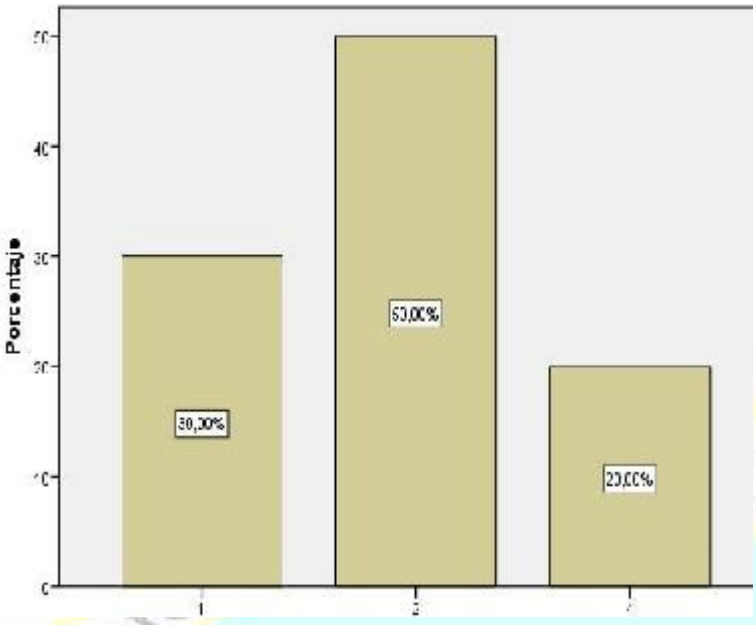


Figura 8. La adecuada configuración de los puertos abiertos aumenta el nivel de vulnerabilidad de los sistemas

En la Tabla 10 y Figura 8, que corresponde al ítem 4, se puede observar que del 100% (30) de trabajadores encuestados, el 50.0% refieren como algo en Desacuerdo, y el 30% están el Total desacuerdo. Por lo tanto, se desprende que el 20% están de acuerdo.

ITEM 5: ¿La evaluación de las Contraseñas mediante la guía de prueba de la Aplicación de Pentesting determina el nivel de seguridad vulnerabilidad del Sistemas de Industrias San Miguel del Sur - Planta Huaura?

Tabla 11

La evaluación de las Contraseñas mediante la guía de prueba de la cación de Pentesting determina el nivel de seguridad vulnerabilidad del mas del Industrias San miguel del sur planta Huaura

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Total desacuerdo	3	10,0	10,0	10,0
	No de acuerdo	12	40,0	40,0	50,0
	De acuerdo	15	50,0	50,0	100,0
	Total	30	100,0	100,0	

Figura 9. La evaluación de las Contraseñas mediante la guía de prueba de la Aplicación de Pentesting determina el nivel de seguridad vulnerabilidad del Sistemas de industrias San Miguel del Sur- Planta Huaura

En la Tabla 11 y Figura 9, que corresponde al ítem 5, se puede observar que del 100% (30) de trabajadores encuestados, el 50% refieren como algo De acuerdo, y el 40 % no están de acuerdo. Por lo tanto, se desprende que el 10% está en Total desacuerdo.

ITEM 6: ¿La guía de prueba de Inyección SQL de la Aplicacion de Pentesting del Sistemas del Industrias San Miguel del Sur - Planta Huaura ayuda a la prevención ataques informáticos

Tabla 12

La guía de prueba de Inyección SQL de la Aplicacion de Pentesting del Sistemas del Industrias San Miguel del sur planta Huaura ayuda a la prevención ataques informáticos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Total desacuerdo	3	10,0	10,0	10,0
	No de acuerdo	3	10,0	10,0	20,0
	De acuerdo	24	80,0	80,0	100,0
	Total	30	100,0	100,0	

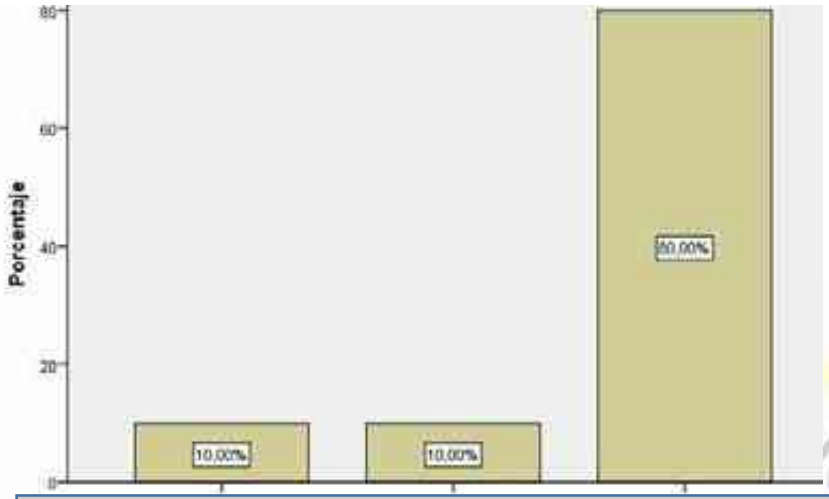


Figura 10. La guía de prueba de Inyección SQL de la aplicación de pentesting del Sistemas de industria san miguel del sur ayuda a la prevención ataques informáticos

INTERPRETACIÓN:

En la Tabla 12 y Figura 10, que corresponde al ítem 6, se puede observar que del 100% (30) de trabajadores encuestados, el 80% refieren como algo De acuerdo, y el 10 % no están de acuerdo. Por lo tanto, se desprende que el 10% está en total desacuerdo.

ITEM 7: La guía de prueba de Inyección SQL de la metodología OWASP, es importante la validación de una consulta SQL con procedimientos almacenados y validaciones de entradas.

Tabla 13

La guía de prueba de Inyección SQL de la Aplicación de Pentesting, es ortante la validación de una consulta SQL con procedimientos acenados y validaciones de entradas.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Total desacuerdo	3	10,0	10,0	10,0
	Desacuerdo	3	10,0	10,0	20,0
	No acuerdo	9	30,0	30,0	50,0
	De acuerdo	15	50,0	50,0	100,0
	Total	30	100,0	100,0	

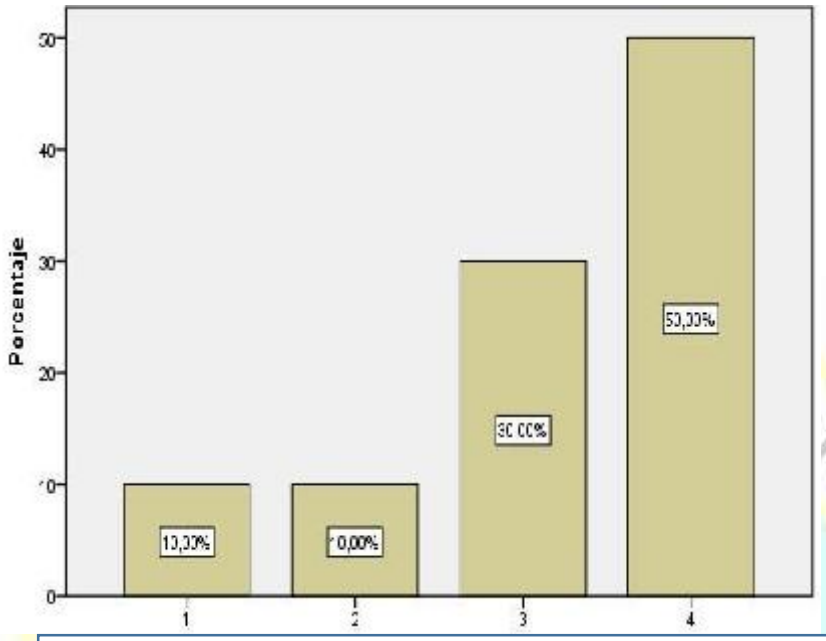


Figura 11. La guía de prueba de Inyección SQL de la aplicación de pentesting es importante la validación de una consulta SQL con procedimientos almacenados y validaciones de entradas.

En la Tabla 13 y Figura 11, que corresponde al ítem 7, se puede observar que del 100% (30) de trabajadores encuestados, el 50% refieren como algo De acuerdo, y el 30 % no están de acuerdo. Por lo tanto, se desprende que el 10% está en desacuerdo y totalmente en desacuerdo.

ITEM 8: La guía de prueba Inclusión de Archivos de la Aplicación de Pentesting previene la vulnerabilidad del Sistemas del Industrias San Miguel del Sur - Planta Huaura

Tabla 14

La guía de prueba Inclusión de Archivos de la Aplicación de Pentesting previene la vulnerabilidad del Sistemas del Industrias San miguel del sur planta Huaura

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Total desacuerdo	9	30,0	30,0	30,0
	No acuerdo	6	20,0	20,0	50,0
	De acuerdo	15	50,0	50,0	100,0
	Total	30	100,0	100,0	

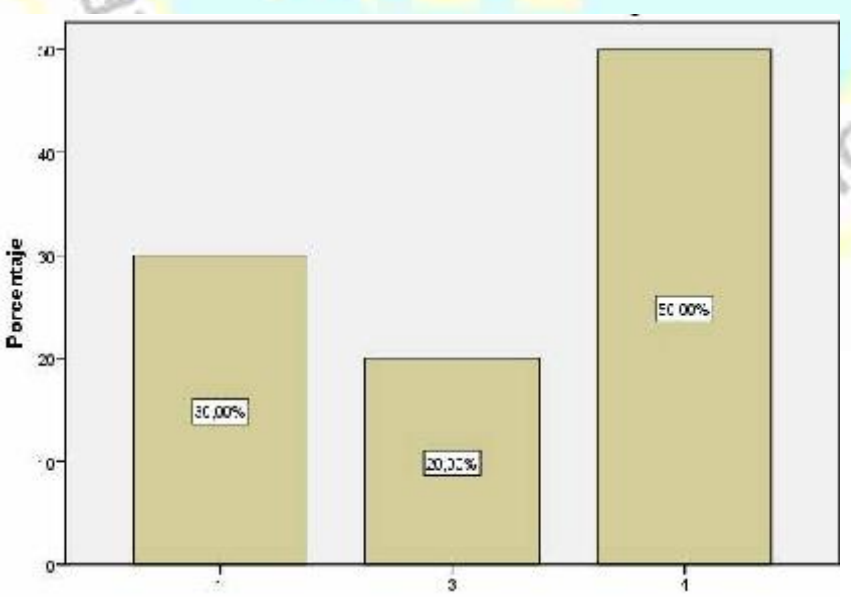


Figura 12. La guía de prueba Inclusión de Archivos de la aplicación de pentesting previene la vulnerabilidad del Sistemas de industrias san miguel planta Huaura

En la Tabla 14 y Figura 12, que corresponde al ítem 8, se puede observar que del 100% (30) de trabajadores encuestados, el 50% refieren como algo De acuerdo, y el 20 % no están de acuerdo. Por lo tanto, se desprende que el 30% está en total desacuerdo.

ITEM 9: La guía de prueba de Algoritmos de la Aplicación de Pentesting previenen la vulnerabilidad del Sistemas del Industrias San Miguel del Sur - Planta Huaura

Tabla 15

La guía de prueba de Algoritmos de la Aplicacion de Pentesting previenen la vulnerabilidad del Sistemas del Industrias San Miguel del sur planta Huaura

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Total desacuerdo	3	10,0	10,0	10,0
	Desacuerdo	6	20,0	20,0	30,0
	No acuerdo	3	10,0	10,0	40,0
	De acuerdo	18	60,0	60,0	100,0
	Total	30	100,0	100,0	

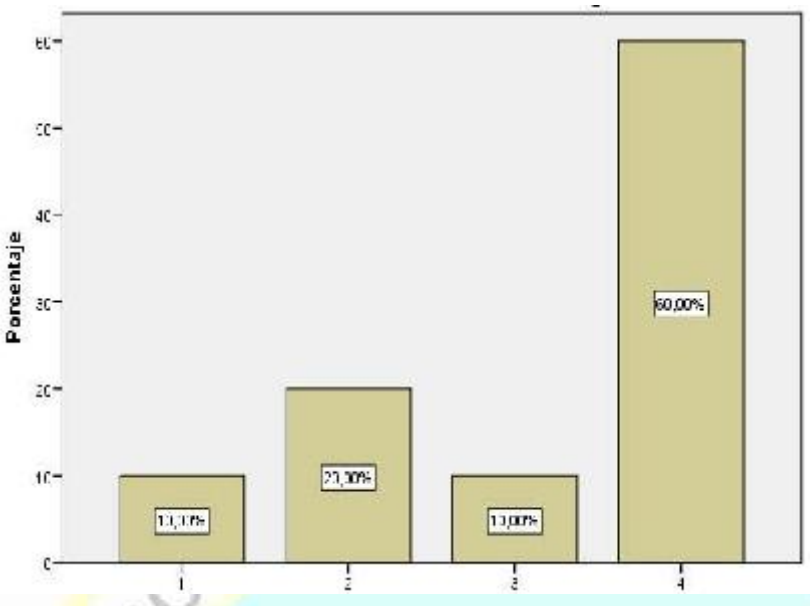


Figura 13. La guía de prueba de Algoritmos de la aplicación de Pentesting previenen la vulnerabilidad del Sistemas de industrias san miguel del sur planta Huaura

En la Tabla 15 y Figura 13, que corresponde al ítem 9, se puede observar que del 100% (30) de trabajadores encuestados, el 60% refieren como algo De acuerdo, y el 20 % están en desacuerdo. Por lo tanto, se desprende que el 10% está en total desacuerdo y no de acuerdo.

ITEM 10: La guía de aplicaciones de Versiones de la Aplicación de Pentesting se relacionan con la prevención de la vulnerabilidad del Sistemas del Industrias San Miguel del Sur - Planta Huaura

Tabla 16

La guía de aplicaciones de Versiones de la Aplicación de Pentesting se relacionan con la prevención de la vulnerabilidad del Sistemas del Industrias San miguel del sur planta Huaura

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Total desacuerdo	3	10,0	10,0	10,0
	No acuerdo	15	50,0	50,0	60,0
	De acuerdo	9	30,0	30,0	90,0
	Total de acuerdo	3	10,0	10,0	100,0
	Total	30	100,0	100,0	

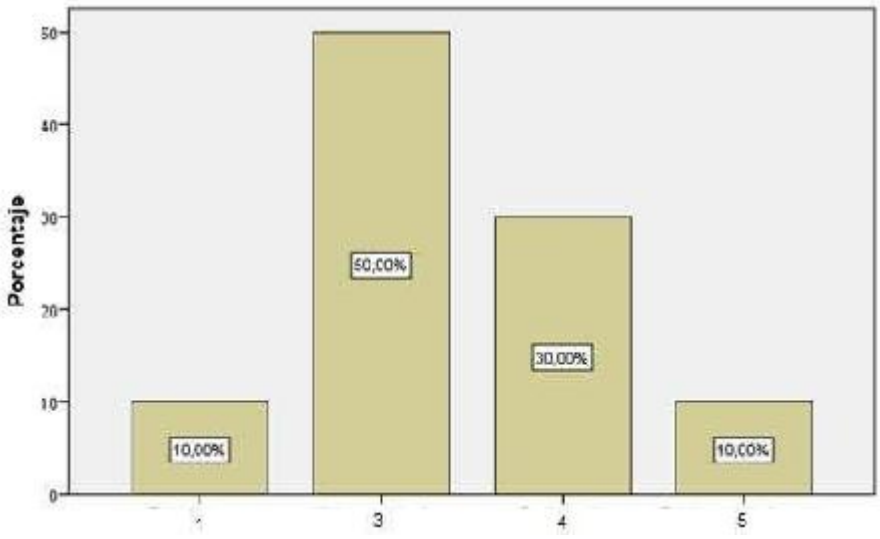


Figura 14. La guía de aplicaciones de Versiones de Pentesting se relaciona con la prevención de la vulnerabilidad del Sistemas de Industrias San Miguel del Sur -Planta Huaura

En la Tabla 16 y Figura 14, que corresponde al ítem 10, se puede observar que del 100% (30) de trabajadores encuestados, el 50% refieren como No De acuerdo, y el 30 % están de acuerdo. Por lo tanto, se desprende que el 10% está en Total desacuerdo Total de acuerdo

ITEM 11: La guía de prueba de Firewall de la Aplicación de Pentesting se relacionan con la prevención de la vulnerabilidad del Sistemas del Industrias San Miguel del sur planta Huaura

Tabla 17

La guía de prueba de Firewall de la Aplicación de Pentesting se relacionan con la prevención de la vulnerabilidad del Sistemas del Industrias San Miguel del Sur - Planta Huaura

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Total desacuerdo	3	10,0	10,0	10,0
	Desacuerdo	3	10,0	10,0	20,0
	No acuerdo	6	20,0	20,0	40,0
	De acuerdo	18	60,0	60,0	100,0
	Total	30	100,0	100,0	

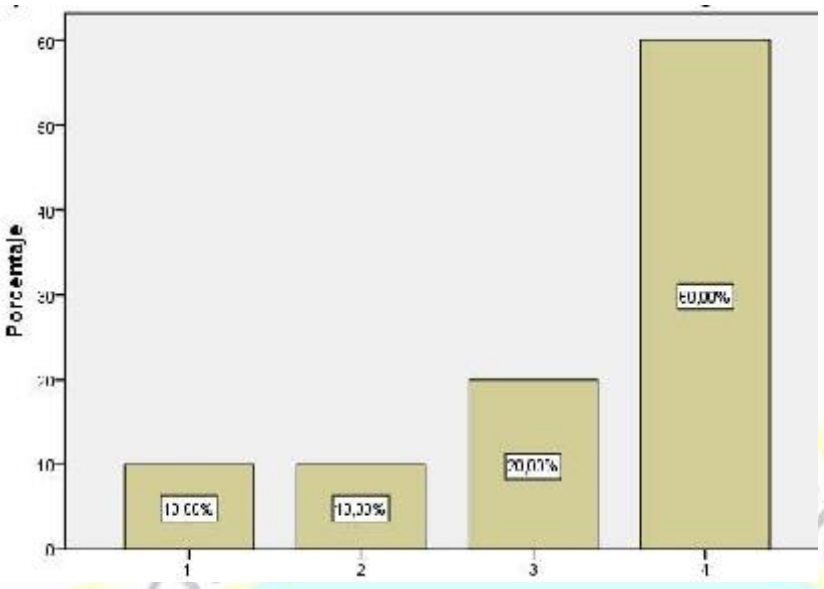


Figura 15 La guía de prueba de Firewall de la aplicación de Pentesting se relaciona con la prevención de la vulnerabilidad del Sistemas de industrias san miguel del sur

En la Tabla 17 y Figura 15, que corresponde al ítem 11, se puede observar que del 100% (30) de trabajadores encuestados, el 60% refieren como algo De acuerdo, y el 20 % no están de acuerdo. Por lo tanto, se desprende que el 10% está en total desacuerdo y desacuerdo.

ITEM 12: La guía de prueba de IDS de la Aplicacion de Pentesting se relacionan con la prevención de la vulnerabilidad del Sistemas del Industrias San Miguel del sur planta Huaura

Tabla 18

La guía de prueba de IDS de la Aplicacion de Pentesting se relacionan con la prevención de la vulnerabilidad del Sistemas del Industrias San Miguel del Sur - Planta Huaura

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Total desacuerdo	3	10,0	10,0	10,0
	Desacuerdo	3	10,0	10,0	20,0
	No acuerdo	9	30,0	30,0	50,0
	De acuerdo	15	50,0	50,0	100,0
	Total	30	100,0	100,0	

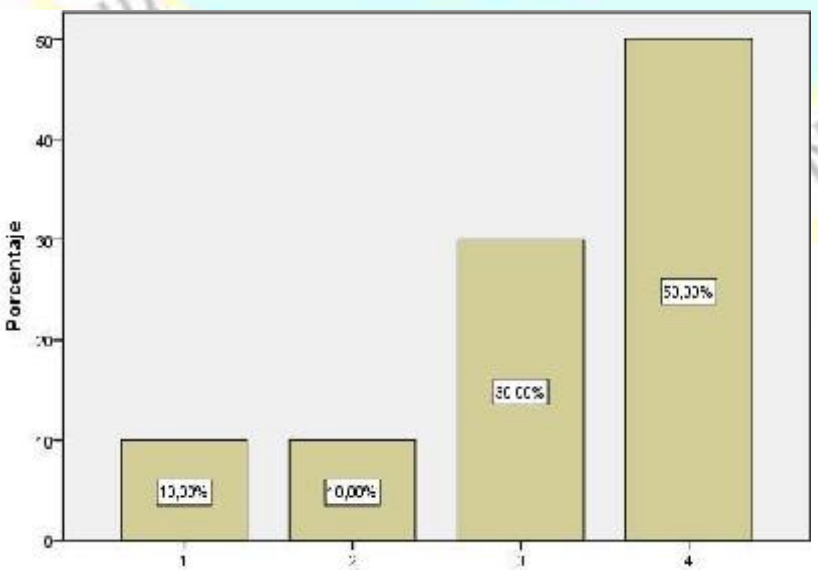


Figura 16. La guía de prueba de IDS de la aplicación de Pentesting se relaciona con la prevención de la vulnerabilidad del Sistemas de industrias San Miguel del Sur Planta Huaura

En la Tabla 18 y Figura 16, que corresponde al ítem 12, se puede observar que del 100% (30) de trabajadores encuestados, el 50% refieren como algo De acuerdo, y el 30 % no están de acuerdo. Por lo tanto, se desprende que el 10% está en desacuerdo y total desacuerdo.

ITEM 13: La implementación de un IDS la seguridad del Sistemas del Industrias San Miguel del Sur - Planta Huaura aumentará la seguridad e integridad.

Tabla 19

La implementación de un IDS la seguridad del Sistemas del Industrias San Miguel del sur planta Huaura aumentará la seguridad e integridad.

Válido Total	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
desacuerdo	3	10,0	10,0	10,0
No acuerdo	3	10,0	10,0	20,0
De acuerdo	24	80,0	80,0	100,0
Total	30	100,0	100,0	

Figura 17. La implementación de un IDS la seguridad del Sistemas de industrias san Miguel del Sur – Planta Huaura aumentará la seguridad e integridad.

En la Tabla 19 y Figura 17, que corresponde al ítem 13, se puede observar que del 100% (30) de trabajadores encuestados, el 80% refieren como algo De acuerdo, y el 10 % no están de acuerdo. Por lo tanto, se desprende que el 10% está en total desacuerdo.

ITEM 14: La implementación de un WAF de la aplicación de Pentesting se relacionan con la prevención de la vulnerabilidad del Sistemas del Industrias San Miguel del Sur - Planta Huaura

Tabla 20

La implementación de un WAF de la Aplicación de Pentesting se relacionan con la prevención de la vulnerabilidad del Sistemas del Industrias San Miguel del Sur - Planta Huaura

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Total desacuerdo	3	10,0	10,0	10,0
	Desacuerdo	3	10,0	10,0	20,0
	De acuerdo	15	50,0	50,0	70,0
	Total desacuerdo	9	30,0	30,0	100,0
	Total	30	100,0	100,0	

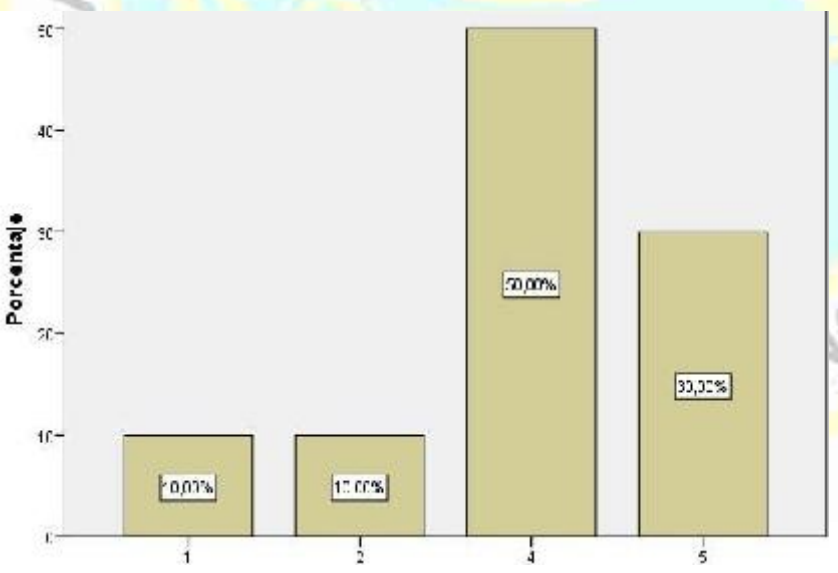


Figura 18. La implementación de un WAF de la Aplicación de Pentesting se relaciona con la prevención de la vulnerabilidad del Sistemas de industrias San Miguel del sur

En la Tabla 20 y Figura 18, que corresponde al ítem 14, se puede observar que del 100% (30) de trabajadores encuestados, el 50% refieren como algo De acuerdo, y el 20 % están en total desacuerdo. Por lo tanto, se desprende que el 10% está en desacuerdo y total desacuerdo.

ITEM 15: La guía de prueba de Rol de Usuario de la Aplicación de Pentesting se relacionan con la prevención de la vulnerabilidad del Sistemas del Industrias San Miguel del Sur – Planta Huaura

Tabla 21

La guía de prueba de Rol de Usuario de la Aplicación de Pentesting se relacionan con la prevención de la vulnerabilidad del Sistemas del Industrias San Miguel del Sur - Planta Huaura

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Total desacuerdo	3	10,0	10,0	10,0
	Desacuerdo	3	10,0	10,0	20,0
	De acuerdo	24	80,0	80,0	100,0
	Total	30	100,0	100,0	

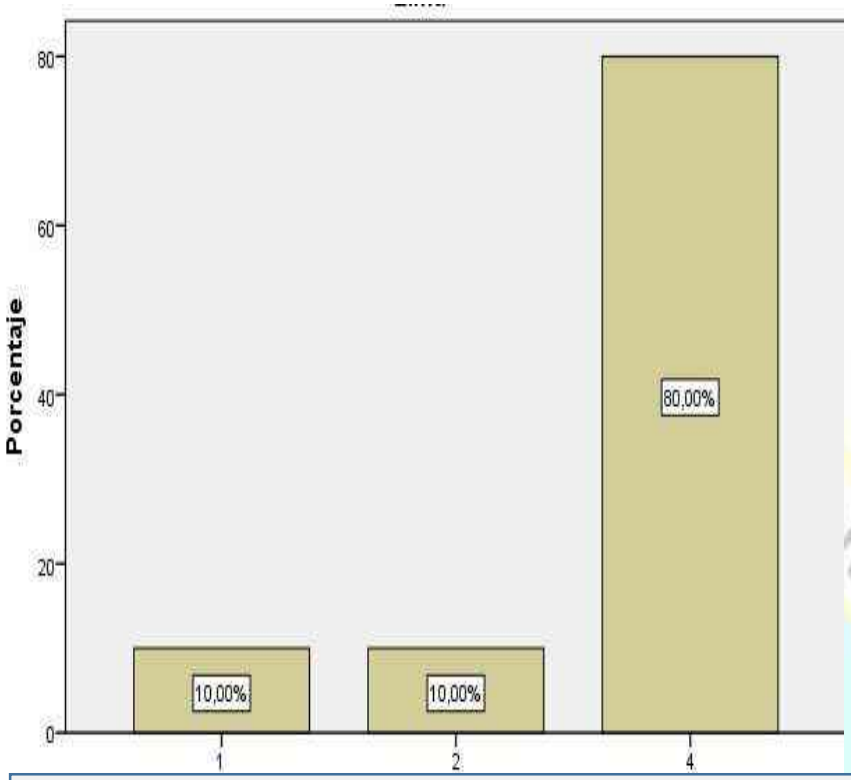


Figura 19. La guía de prueba de Rol de Usuario de la aplicación de Pentesting se relaciona con la prevención de la vulnerabilidad del Sistemas de industrias San Miguel del Sur- Planta Huaura

En la Tabla 21 y Figura 19, que corresponde al ítem 15, se puede observar que del 100% (30) de trabajadores encuestados, el 70% refieren como algo De acuerdo, y el 20 % no están de acuerdo. Por lo tanto, se desprende que el 10% está en desacuerdo.

4.2.4 Contrastación de hipótesis

Luego de la recolección de los datos se pasó al análisis de ellos según las hipótesis generales y especificas planteadas. La metodología que se siguió consiste en hacer una comparación entre las dimensiones y luego pasar a una comparación de las variables dependientes e independientes. Se aplicó la Prueba Paramétrica de

Coeficiente de Pearson de acuerdo a los resultados obtenidos de la prueba de Kolmogorov-Smirnov y además queremos conocer el grado de asociación, así como también el saber si esta es positiva o negativa.

HIPÓTESIS GENERAL

Ha: □□ 0: La **Aplicación de Pentesting**, se relaciona significativamente con los **Sistemas del** *Industrias San Miguel del Sur*

.

H0: □ = 0: La **Aplicación de Pentesting**, No se relaciona significativamente con los **Sistemas** *del Industrias San Miguel del Sur planta Huaura*

PRUEBA DE LA HIPÓTESIS GENERAL

A. HIPÓTESIS ESTADÍSTICA

El valor de coeficiente de correlación r de Spearman determina una relación lineal entre las variables ordinales o nominales; nos indica si esta relación es estadísticamente significativa.

$$r_S = 1 - \frac{6 \sum D_i^2}{N^3 - N}$$

Donde:

D*i*: Diferencia entre el i-ésimo par de rangos = $R(X_i)-R(Y_i)$

$R(X_i)$: es el rango del i-ésimo dato X

$R(Y_i)$: es el rango del i-ésimo dato Y

N: es el número de parejas de rangos

El valor rs de Spearman es $r_s = 0,766$

B. PRUEBA DE HIPÓTESIS

Para ello, se aplica la prueba de hipótesis de parámetro ρ (rho).

Como en toda prueba de hipótesis, la hipótesis nula H_0 establece que no existe una relación, es decir, que el coeficiente de correlación ρ es igual a 0. Mientras que la hipótesis alterna H_a propone que sí existe una relación significativa, por lo que ρ debe ser diferente a 0.

Ho: ρ = 0 **H_a: ρ ≠ 0**

C. DECISIÓN ESTADÍSTICA:

Tabla 20

Prueba de hipótesis general

			Aplicación de Pentesting	Sistemas
Rho de Spearman	**Aplicación de Pentesting**	Coeficiente de correlación	1,000	0,766**
		Sig. (bilateral)	.	0,000
		N	30	30
	Sistemas	Coeficiente de correlación	0,766**	1,000
		Sig. (bilateral)	0,000	.
		N	30	30

**. La correlación es significativa al nivel 0,01 (bilateral).

De acuerdo al resultado del procesamiento obtenido con el SPSS 23, se puede observar una alta correlación entre ambas variables que arroja el coeficiente de Spearman igual a 0.766. Para la contrastación de la hipótesis se realiza el análisis de p valor o sig. Asintótica (Bilateral) = 0.000 que es menor que 0.05, por lo que se niega la hipótesis nula y por consiguiente se acepta la Ha.

D. RESULTADO:

Se concluye en el rechazo de la hipótesis nula y la aceptación de la hipótesis general alterna.

PRUEBA DE LAS HIPÓTESIS ESPECÍFICAS

A. Hipótesis específica H_1

H_1: *Existe relación significativa entre la configuración y la prevención de ataques a los sistemas del Industrias San Miguel del Sur planta Huaura.*

H_0: No *Existe relación significativa entre la configuración y la prevención de ataques a los sistemas del Industrias San Miguel del Sur planta Huaura.*

HIPÓTESIS ESTADÍSTICA

El valor de coeficiente de correlación r de Spearman determina una relación lineal entre las variables ordinales o nominales; nos indica si esta relación es estadísticamente significativa.

$$r_S = 1 - \frac{6 \sum D_i^2}{N^3 - N}$$

El valor de spearman es $r_s = 0{,}633$

Para ello, se aplica la prueba de hipótesis de parámetro ρ (rho). Como en toda prueba de hipótesis, la hipótesis nula H_0 establece que no existe una mejora, es decir, que el coeficiente de correlación ρ es igual a 0. Mientras que la hipótesis alterna H_1 propone que sí existe una mejora significativa, por lo que ρ debe ser diferente a 0.

Ho: $\rho = 0$ **H_1: $\rho \neq 0$**

Tabla 21

Prueba de hipótesis específica 1

			Aplicación de Pentesting	Sistemas
Rho de Spearman	**Aplicación de Pentesting**	Coeficiente de correlación	1,000	0,633**
		Sig. (bilateral)	.	0,000
		N	30	30
	Sistemas	Coeficiente de correlación	0,633**	1,000
		Sig. (bilateral)	0,000	.
		N	30	30

**. La correlación es significativa al nivel 0,01 (bilateral).

DECISIÓN ESTADÍSTICA

De acuerdo al resultado del procesamiento obtenido con el SPSS 23, se puede observar una buena correlación entre ambas variables que arroja el coeficiente de Spearman igual a 0.633. Para la contrastación de la hipótesis se realiza el análisis de p valor o sig. Asintótica (Bilateral) = 0.000 que es menor que 0.05, por lo que se niega la hipótesis nula y por consiguiente se acepta la H_1.

RESULTADO:

Se concluye en el rechazo de la hipótesis nula y la aceptación de la hipótesis alterna H_1.

B. Prueba de la hipótesis específica H_2:

H_2: *Existe relación significativa entre la configuración y la prevención de ataques a los sistemas del Industrias San Miguel del Sur planta Huaura.*

H_0: No *Existe relación significativa entre la configuración y la prevención de ataques a los sistemas del Industrias San Miguel del Sur planta Huaura.*

HIPÓTESIS ESTADÍSTICA:

El valor de coeficiente de correlación r de Spearman determina una relación lineal entre las variables ordinales o nominales; nos indica si esta relación es estadísticamente significativa.

$$r_S = 1 - \frac{6 \sum D_i^2}{N^3 - N}$$

El valor rs de Spearman es $r_s = 0{,}656$.

Para ello, se aplica la prueba de hipótesis de parámetro ρ (rho). Como en toda prueba de hipótesis, la hipótesis nula H_0 establece que no existe una Mejora, es decir, que el coeficiente de correlación ρ es igual a 0. Mientras que la hipótesis alterna H_2 propone que sí existe una Mejora significativa, por lo que ρ debe ser diferente a 0.

H_o: $\rho = 0$ **H_2: $\rho \neq 0$**

Tabla 22

Prueba de hipótesis especifica 2

			Aplicación de Pentesting	Sistemas
Rho de Spearman	**Aplicación de Pentesting**	Coeficiente de correlación	1,000	0,656**
		Sig. (bilateral)	.	0,000
		N	30	30
	Sistemas	Coeficiente de correlación	0,656**	1,000
		Sig. (bilateral)	0,000	.
		N	30	30

**. La correlación es significativa al nivel 0,01 (bilateral).

DECISIÓN ESTADÍSTICA:

De acuerdo al resultado del procesamiento obtenido con el SPSS 23, se puede observar una buena correlación entre ambas variables que arroja el coeficiente de Spearman igual a 0,656. Para la contrastación de la hipótesis se realiza el análisis de p valor o sig. Asintótica (Bilateral) = 0,00 que es menor que 0,05, por lo que se niega la hipótesis nula y por consiguiente se acepta la H_2.

RESULTADO:

Se concluye en el rechazo de la hipótesis nula y la aceptación de la hipótesis alterna H_2.

B. Prueba de la hipótesis específica H_3:

H_3: *Existe relación significativa entre la criptografía y la prevención de ataques a los sistemas del Industrias San Miguel del Sur planta Huaura*

H_0: No *Existe relación significativa entre la criptografía y la prevención de ataques a los sistemas del Industrias San Miguel del Sur planta Huaura*

HIPÓTESIS ESTADÍSTICA:

El valor de coeficiente de correlación r de Spearman determina una relación lineal entre las variables ordinales o nominales; nos indica si esta relación es estadísticamente significativa.

$$r_S = 1 - \frac{6 \sum D_i^2}{N^3 - N}$$

El valor rs de Spearman es $r_s = 0{,}678$.

Para ello, se aplica la prueba de hipótesis de parámetro ρ (rho). Como en toda prueba de hipótesis, la hipótesis nula H_0 establece que no existe una Mejora, es decir, que el coeficiente de correlación ρ es igual a 0. Mientras que la hipótesis alterna H_3 propone que sí existe una relación significativa, por lo que ρ debe ser diferente a 0.

H_o: $\rho = 0$ **H_3: $\rho \neq 0$**

Tabla 23

Prueba de hipótesis especifica 3

			Aplicación de Pentesting	Sistemas
Rho de Spearman	**Aplicación de Pentesting**	Coeficiente de correlación	1,000	0,678**
		Sig. (bilateral)	.	0,000
		N	30	30
	Sistemas	Coeficiente de correlación	0,678**	1,000
		Sig. (bilateral)	0,000	.
		N	30	30

**. La correlación es significativa al nivel 0,01 (bilateral).

DECISIÓN ESTADÍSTICA:

De acuerdo al resultado del procesamiento obtenido con el SPSS 23, se puede observar una buena correlación entre ambas variables que arroja el coeficiente de Spearman igual a 0,678. Para la contrastación de la hipótesis se realiza el análisis de p valor o sig. Asintótica (Bilateral) = 0,00 que es menor que 0,05, por lo que se niega la hipótesis nula y por consiguiente se acepta la $H_{3.}$

RESULTADO:

Se concluye en el rechazo de la hipótesis nula y la aceptación de la hipótesis alterna $H_{3.}$

POR LO TANTO:

En las tres pruebas de hipótesis específicas y la hipótesis general, se encuentra que en su totalidad se Acepta la Hipótesis Alternativa, dando paso al rechazo de la Hipótesis Nula, con lo que se confirma la ACEPTACIÓN DE LA HIPÓTESIS PRINCIPAL, es decir que: La **Aplicación de Pentesting**, se relaciona significativamente con **los sistemas del Industrias San Miguel del Sur planta Huaura.**

CAPÍTULO V

DISCUSIÓN

5.1 Discusión de resultados

Comparando con los antecedentes de la investigación considerados en la presente tesis en líneas generales concedimos son los resultados obtenidos como se puede apreciar en las conclusiones de los autores de la tesis más importante:

Aguilar, V. (2015), Concluyo que se desarrolló la evaluación de ethical hacking de lasolución propuesta en la Caja Municipal de Sullana lográndose descubrir todas las vulnerabilidades que surgen, las mismas que se reprendieron, permaneciendo autónomo de errores, el cual optimiza la seguridad y da confianza a la gerencia en el uso de sistemas y redes de datos.

Se realizó la solución al problema de la seguridad, se implementó una solución de hacking ético en la infraestructura informática de la Caja Municipal de Sullana - Agencia Chimbote, con lo cual se mejoró la seguridad en la transferencia de datos.

Díaz J., Antonio L. y Salcedo J. (2013) Concluyo que las vulnerabilidades nos indican que en un sistema existe debilidad, ello consentirá a un hacker o cracker desarrollar un ataque y quebrantar la confidencialidad, disponibilidad e integridad. En la actualidad muchos de los sistemas de información de una empresa se encuentran interconectados entre diferentes computadoras o subidos a la WEB y para la accesibilidad y el desarrollo laboral entre diferentes áreas de trabajo, estas conexiones entre computadoras son conocidas como REDS LAN.

Huilca, Gloria (2018). Concluyo que un proyecto de Hacking Ético reside en una inserción en los sistemas informáticos de una compañía, del mismo modo que lo realizaría un pirata informático o hacker, sin embargo de manera ética, previa autorización. El objetivo elemental de la aplicación de hacking ético es revelar las insuficiencias concernientes a la

seguridad y las vulnerabilidades de los sistemas informáticos, estudiarlas, calibrar su nivel de riesgo y peligro, y encomendar las posibles soluciones más adecuadas para cada uno de ellos. Por dicho origen es de mucha importancia usar el Hacking Ético en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos para descubrir vulnerabilidades, de tal modo se descubrió a tiempo las vulnerabilidades existentes, ofrecer probables soluciones para procurar aseverar los servicios y por ello lograr favorecer al Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos obteniendo ofrecer unos servicios de calidad y seguridad esencialmente a un grado de transmisión de información en la intranet.

Mediante la investigación que he realizado concluyo, que existe una elación directa y significativa entre la Aplicación de pentesting y la prevención de ataques a los sistemas de Industrias San Miguel Del Sur – Planta Huaura 2019 ambas variables que proyecta el coeficiente de Spearman igual a 0.766. Para la contrastación de la hipótesis se realiza el análisis de p valor o sig. Asintótica (Bilateral) = 0.000 que es menor que 0.05, por lo que se niega la hipótesis nula y por consiguiente se acepta la Ha.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

a) Se concluye una alta correlación entre la aplicación de pentesting y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019 que arroja el coeficiente de Spearman igual a 0.766. Con p valor o sig. Asintótica (Bilateral) = 0.000 que es menor que 0.05, por lo que se rechaza la hipótesis nula y por consiguiente se acepta la alterna del investigador.

b) Se observar una buena correlación entre las variables configuración y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019. que arroja el coeficiente de Spearman igual a 0.633. Con de p valor o sig. Asintótica (Bilateral) = 0.000 que es menor que 0.05, por lo que se rechaza la hipótesis nula y por consiguiente se acepta la hipótesis alterna del investigador.

c) Se concluye una buena correlación entre variables entre la prueba de caja negra y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019, cuyo resultado arroja el coeficiente de Spearman igual a 0,656. Con p valor o sig. Asintótica (Bilateral) = 0,00 que es menor que 0,05, por lo que se rechaza la hipótesis nula y por consiguiente se acepta la hipótesis alterna del investigador.

d) Igualmente se concluye una buena correlación entre las variables la prueba de criptografía y la prevención de ataques a los sistemas de Industrias San Miguel del Sur –

Planta Huaura, año 2019, cuyo resultado arroja el coeficiente de Spearman igual a 0,678. con de p valor o sig. Asintótica (Bilateral) = 0,00 que es menor que 0,05, por lo que se rechaza la hipótesis nula y por consiguiente se acepta la hipótesis alterna del investigador.

6.2 Recomendaciones

a) Se recomienda a los directivos de la organización a realizar los estudios para llevar a cabo la Implementación de la Aplicación de Pentesting para prevención de ataques a los sistemas web del Industrias San miguel del Sur-Planta Huaura, con un estudio aplicativo a fin de enfocar la seguridad de aplicaciones informáticas considerando todas sus dimensiones: personas, procesos y tecnologías.

b) Se recomienda al Jefe de la Oficina de informática de la Empresa Industrias San Miguel del Sur – Planta Huaura a capacitar permanentemente en seguridad informática, para garantizar la seguridad integridad y disponibilidad de los sistemas.

c) Ejecutar pruebas de Pentesting a nivel perimetral anualmente como en la implementación de una solución informática de área de informática de ISM en fase producción ya que esto nos dará indicadores KPIS y tente respuesta de mitigación ante un ataque informático que con el devenir del tiempo ha crecido estos últimos tiempos.

REFERENCIAS

7.1 Fuentes documentales

No se utilizó ninguna fuente documental

7.2 Fuentes bibliográficas

Aguilera, P. (2011). *Redes seguras (Seguridad informática)* (9ª Ed.). México: Mc Graw Hill.

Aguila.S. Vilky, G. De la Cruz V. (2015). Implementación de una Solución Hacking ético para Mejorar la seguridad en la Infraestructura Informática de la Caja Municipal de Sullana. Tesis. Chimbote: Universidad Nacional del Santa.

Blanchard, B. S. (1995). *Ingeniería de sistemas*. (8ª Ed.). México: Mc Graw Hill.

Crespo, E. (2013) Hacking ético para pymes. Tesis. Ecuador: Universidad de Azuay.

Díaz, J. Salcedo, S. (2013). Sistema de Prevención de Intrusos para Mejorar la Seguridad de los Servicios de la Universidad Nacional de Trujillo. Tesis. Trujillo: Universidad Nacional de Trujillo.

Gonzales, C. Bernier. (2016). Uso de Herramientas de Ethical Hacking con Kalinux para el Diagnostico de Vulnerabilidades en la Seguridad de la Información en la red del sede Central de la Universidad de Huánuco. Tesis. Huanuco: Universidad Nacional de Huanuco.

Griffin, R. (2011). *Administración* (10ª Ed.). México: Cengage Learning.

Hernández, R.; Fernández, C. & Baptista, P. (2014). *Metodología de la Investigación* (6ª Ed.) México: Mc Graw Hill.

Huilca, G. (2009). Hacking ético para detectar vulnerabilidades en los servicios de intranet del gobierno autónomo descentralizado municipal Canton Cevallos. Tesis. Ecuador: Escuela Politécnica Ambato Nacional.

Marañon, G. Á., García, P. & Bustamante, P. (2004) *Seguridad informática para la empresa.* México: Mc Graw Hill.

Pazmiño, A. (2011). *Aplicación de hacking ético para la determinación de vulnerabilidades de acceso a redes inalámbricos wifi. Tesis. Ecuador: Escuela Superior Politécnica de Chimborazo.*

Vidal Ledo, M., Fernández Oliva, B., Alfonso Sánchez, I. R., & Armenteros Vera, I. (2004). *Información, informática y estadísticas: un perfil de la Tecnología. Revista de Tecnología.*

Gordillo López, P. L. (2016). *Simulación de un perímetro de seguridad lógica empleando nueva generación de Firewalls para prevenir ataques externos e internos a la granja de servidores de un proveedor de servicios de Internet en una red IP-MPLS*

7.3 Fuentes hemerográficas

7.4 Fuentes electrónicas

Díaz J. (2013) *Sistema de prevención de intrusos para mejorar la seguridad de los servidores de la universidad nacional de Trujillo*. Universidad Nacional de Trujillo. Perú. Recuperado el 15 de Julio del 2018, de http://repositorio.uns.edu.pe/bitstream/handle/UNS/1964/30710.pdf?sequence=1

Huilca C. y Gloria N.(2010). *Utilización de hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones. Ecuador. Recuperado el 20 de Julio del 2018*

https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf?sequence

Verdesoto A. (2007).*Utilización de hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones Ecuador Recuperado 30 de Agosto del 2018* http://bibdigital.epn.edu.ec/handle/15000/548

ANEXOS

Cuestionario de Encuesta

I. PRESENTACIÓN

Estimado (a) señor (a), el presente cuestionario es parte de una investigación que tiene por finalidad obtener información, acerca de la Recolección de datos para las Variables

II. INSTRUCCIONES

- Este cuestionario es anónimo. Por favor responda con sinceridad.
- Escriba a que área pertenece, lea detenidamente cada ítem. Responda el ítem y ponga una escala valorativa que se muestra en el cuadro.
- Gracias por su colaboración.

Área: _____

Escala valorativa

T.E.D	E.D.A	N.S/N.O.	D.A.	**T.D.A.**
1	**2**	**3**	**4**	**5**

PREGUNTAS	T.E.D	E.D.A	N.S/N.O.	D.A.	T.D.A.
1. ¿El Conocimiento que tiene respecto a la vulnerabilidad de los sistemas web, permite detectarlos con facilidad en Industrias san miguel del sur?					
2. ¿El Motor de base de datos de la metodología pentesting aplicado, previene la vulnerabilidad del Sistemas web de industrias san miguel del sur?					
3. ¿La Implementación del procedimiento almacenado y triggers en el Motor de base de datos detecta la intrusión en los sistemas de industrias san miguel del sur ?					
4. ¿La adecuada configuración de los puertos abiertos, aumenta el nivel de vulnerabilidad de los sistemas?					
5. ¿La evaluación de las Contraseñas mediante la guía de prueba de pentesting determina el nivel de seguridad vulnerabilidad industrias san miguel del sur ?					
6. ¿La guía de prueba de Inyección SQL de pentesting de industrias san miguel del sur ayuda a la prevención ataques informáticos?					
7. ¿La guía de prueba de Inyección SQL de pentesting, es importante la validación de una consulta SQL con procedimientos almacenados y validaciones de entradas?					
8. ¿La guía de prueba Inclusión de Archivos de pentesting P previene la vulnerabilidad del Sistemas web de industrias san miguel del sur ?					
9. ¿La guía de prueba de Algoritmos de pentesting previenen la vulnerabilidad del Sistemas de industrias san miguel del sur ?					

10. ¿La guía de aplicaciones de Versiones de pentesting se relacionan con la prevención de la vulnerabilidad del Sistemas de industrias san miguel del sur ?					
11. ¿La guía de prueba de Firewall de pentesting se relacionan con la prevención de la vulnerabilidad del Sistemas de industrias san miguel del sur ?					
12. ¿La guía de prueba de IDS de pentesting se relacionan con la prevención de la vulnerabilidad del Sistemas de industrias san miguel del sur ?					
13. ¿La implementación de un IDS la seguridad del Sistemas de industrias san miguel del sur aumentará la seguridad e integridad?					
14. ¿La implementación de un WAF de pentesting se relacionan con la prevención de la vulnerabilidad del Sistemas de industrias san miguel del sur ?					
15. ¿La guía de prueba de Rol de Usuario de pentesting se relacionan con la prevención de la vulnerabilidad del Sistemas de industrias san miguel del sur ?					

ANEXO - Matriz de consistencia

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLE	DIMENSIONES	METODOLOGÍA
PROBLEMA PRINCIPAL ¿De qué manera la aplicación de pentesting se relaciona con la prevención de ataques a los sistemas de Industrias San Miguel del Sur- Planta Huaura, año 2019? **PROBLEMAS ESPECÍFICOS** a) ¿Qué relación existe entre la configuración y la prevención de ataques a los sistemas de Industrias San Miguel del Sur -Planta Huaura, año 2019? b) ¿Qué relación existe entre la prueba de caja negra y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019? c) ¿Qué relación existe entre la prueba de criptografía y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019?	**OBJETIVO GENERAL** Determinar de qué manera la aplicación de pentesting se relaciona con la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019. **OBJETIVOS ESPECÍFICOS** a) Determinar la relación entre la configuración y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019. b) Determinar la relación entre la caja negra y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019. c) Determinar la relación entre la criptografía y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019.	**HIPÓTESIS GENERAL** La aplicación de pentesting se relaciona significativamente con la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura, año 2019 **HIPÓTESIS ESPECÍFICOS** a) Existe relación significativa entre la configuración y la prevención de ataques a los sistemas de Industrias San Miguel del Sur -Planta Huaura, año 2019. b) Existe relación significativa entre la caja negra y la prevención de ataques a los sistemas de Industrias San Miguel del Sur -Planta Huaura, año 2019. c) Existe relación significativa entre la criptografía y la prevención de ataques a los sistemas de Industrias San Miguel del Sur -Planta Huaura, año 2019.	**Variable I:** Aplicación de Pentesting **Variable II:** Prevención de Ataques a los sistemas	1.1. Configuración 1.2. Pruebas de Caja Negra 1.3. Criptografía 2.1. Actualización 2.2. Preventor 2.3. Administración de Privilegios	**POBLACIÓN** La población estará constituida por 30 trabajadores de la oficina informática **MUESTRA** Considerando que la población es pequeña se realizara una muestra censal **NIVEL DE INVESTIGACIÓN:** Correlacional **DISEÑO DE INVESTIGACIÓN:** No experimental, descriptiva y Correlacional. **TIPO DE INVESTIGACIÓN:** Aplicada **ENFOQUE DE LA INVESTIGACIÓN** Cuantitativo **TÉCNICA DE LA RECOPILACIÓN DE DATOS** La encuesta **INSTRUMENTO DE LA RECOPILACIÓN DE DATOS** Cuestionario de la encuesta Escala de Likert **TÉCNICA DE PROCESAMIENTO DE LA INFORMACIÓN** Software SPSS 23

UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

INFORME DE JUICIO DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

TITULO: APLICACIÓN DE PENTESTING Y PREVENCIÓN DE ATAQUES A LOS SISTEMAS DE INDUSTRIAS SAN MIGUEL DEL SUR – PLANTA HUAURA, AÑO 2019

AUTOR DEL INSTRUMENTO: Hector Angel Mena Bernal

II ASPECTOS DE VALIDACION

INDICADORES	CRITERIOS	DEFICIENTE				REGULAR				BUENA				MUY BUENA				EXCELENTE			
		0	4	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
01. CLARIDAD	Está formulado con lenguaje apropiado.																	85			
02. OBJETIVIDAD	Está expresado en hechos observables.																	85			
03. ACTUALIDAD	Adecuado al avance de la tecnología.																	85			
04. ORGANIZACIÓN	Existe una organización lógica.																	85			
05. SUFICIENCIA	Comprende los aspectos en cantidad y calidad.																	85			
06. INTENCIONALIDAD	Adecuado para valorar los aspectos de los administradores de la unidad de Usuarios.																	85			
07. CONSISTENCIA	Basado en aspectos teóricos científicos.																	85			
08. COHERENCIA	Entre los objetivos, hipótesis e indicadores.																	85			
09. METODOLOGÍA	La estrategia responde a los objetivos de																	85			
10. PERTINENCIA	Es útil y adecuado para la investigación																	85			

I. OPINIÓN DE LA APLICABILIDAD: EXCELENTE

II. PROMEDIO DE VALORACIÓN: 85%

Firma del experto informante

Apellidos y Nombres: PALOMINO TIÑADO, M.

DNI Nº 08719903

6

INFORME DE JUICIO DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

TITULO: APLICACIÓN DE PENTESTING Y PREVENCIÓN DE ATAQUES A LOS SISTEMAS DE INDUSTRIAS SAN MIGUEL DEL SUR – PLANTA HUAURA, AÑO 2019

AUTOR DEL INSTRUMENTO: Hector Angel Mena Bernal

II. ASPECTOS DE VALIDACION

INDICADORES	CRITERIOS	DEFICIENTE				REGULAR				BUENA				MUY BUENA				EXCELENTE			
		0-5	6-10	11-15	16-20	21-25	26-30	31-35	36-40	41-45	46-50	51-55	56-60	61-65	66-70	71-75	76-80	81-85	86-90	91-95	96-100
11. CLARIDAD	Está formulado con lenguaje apropiado.																X				
12. OBJETIVIDAD	Está expresado en hechos observables.																	X			
13. ACTUALIDAD	Adecuado al avance de la tecnología.																	X			
14. ORGANIZACIÓN	Existe una organización lógica.																	X			
15. SUFICIENCIA	Comprende los aspectos en cantidad y calidad.																	X			
16. INTENCIONALIDAD	Adecuado para valorar los aspectos de los administrativos de la unidad de sistemas.																	X			
17. CONSISTENCIA	Basado en aspectos teóricos científicos.																X				
18. COHERENCIA	Entre los objetivos, hipótesis e indicadores.																	X			
19. METODOLOGÍA	La estrategia responde a los objetivos de																X				
20. PERTINENCIA	Es útil y adecuado para la investigación																	X			

II. OPINIÓN DE LA APLICABILIDAD: Cabe

III. PROMEDIO DE VALORACIÓN: 83,5

Firma del experto informante:

Apellidos y Nombres: Pérez Ramírez José Luis

DNI Nº 15532348

INFORME DE JUICIO DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

TITULO: APLICACIÓN DE PENTESTING Y PREVENCIÓN DE ATAQUES A LOS SISTEMAS DE INDUSTRIAS SAN MIGUEL DEL SUR – PLANTA HUAURA, AÑO 2019

AUTOR DEL INSTRUMENTO: Hector Angel Mena Bernal

II. ASPECTOS DE VALIDACION

INDICADORES	CRITERIOS	DEFICIENTE				REGULAR				BUENA				MUY BUENA				EXCELENTE			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
11. CLARIDAD	Está formulado con lenguaje apropiado.																X				
12. OBJETIVIDAD	Está expresado en hechos observables.																X	X			
13. ACTUALIDAD	Adecuado al avance de la tecnología.																	X			
14. ORGANIZACIÓN	Existe una organización lógica.																	X			
15. SUFICIENCIA	Comprende los aspectos en cantidad y calidad.																	X			
16. INTENCIONALIDAD	Adecuado para valorar los aspectos de los administrativos de la unidad de sistemas																	X			
17. CONSISTENCIA	Basado en aspectos teóricos científicos																X				
18. COHERENCIA	Entre los objetivos, hipótesis e indicadores.																	X			
19. METODOLOGÍA	La estrategia responde a los objetivos de																	X			
20. PERTINENCIA	Es útil y adecuado para la investigación																	X			

II. OPINIÓN DE LA APLICABILIDAD: Excelente

III. PROMEDIO DE VALORACIÓN: 82.5

Firma del experto informante:

Apellidos y Nombres: CHAVEZ ZAVALETA, RAUL

DNI Nº 10765451

INFORME DE JUICIO DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

TITULO: APLICACIÓN DE PENTESTING Y PREVENCIÓN DE ATAQUES A LOS SISTEMAS DE INDUSTRIAS SAN MIGUEL DEL SUR – PLANTA HUAURA, AÑO 2019

AUTOR DEL INSTRUMENTO: Hector Angel Mena Bernal

II. ASPECTOS DE VALIDACION

INDICADORES	CRITERIOS	DEFICIENTE				REGULAR				BUENA				MUY BUENA				EXCELENTE			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
11. CLARIDAD	Está formulado con lenguaje apropiado.																	X			
12. OBJETIVIDAD	Está expresado en hechos observables.																	X			
13. ACTUALIDAD	Adecuado al avance de la tecnología.																X				
14. ORGANIZACIÓN	Existe una organización lógica.																	X			
15. SUFICIENCIA	Comprende los aspectos en cantidad y calidad.																X				
16. INTENCIONALIDAD	Adecuado para valorar los aspectos de los administrativos de la unidad de sistemas																	X			
17. CONSISTENCIA	Basado en aspectos teóricos científicos																	X			
18. COHERENCIA	Entre los objetivos, hipótesis e indicadores.																X				
19. METODOLOGÍA	La estrategia responde a los objetivos de																	X			
20. PERTINENCIA	Es útil y adecuado para la investigación																	X			

II. OPINIÓN DE LA APLICABILIDAD: Colinde

III. PROMEDIO DE VALORACIÓN: 5.1

Firma del experto informante

Apellidos y Nombres: MANRIQUE QUISPE B, JAVIER ALBERTO

DNI N°: 15640920

INFORME DE JUICIO DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

TITULO: APLICACIÓN DE PENTESTING Y PREVENCIÓN DE ATAQUES A LOS SISTEMAS DE INDUSTRIAS SAN MIGUEL DEL SUR – PLANTA HUAURA, AÑO 2019

AUTOR DEL INSTRUMENTO: Hector Angel Mena Bernal

II. ASPECTOS DE VALIDACION

INDICADORES	CRITERIOS	DEFICIENTE				REGULAR				BUENA				MUY BUENA				EXCELENTE			
		0	6	11	15	21	25	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
11. CLARIDAD	Está formulado con lenguaje apropiado.																X				
12. OBJETIVIDAD	Está expresado en hechos observables.																	X			
13. ACTUALIDAD	Adecuado al avance de la tecnología.																	X			
14. ORGANIZACIÓN	Existe una organización lógica.																X				
15. SUFICIENCIA	Comprende los aspectos en cantidad y calidad.																	X			
16. INTENCIONALIDAD	Adecuado para valorar los aspectos de los administrativos de la unidad de sistemas																X				
17. CONSISTENCIA	Basado en aspectos teóricos científicos																X				
18. COHERENCIA	Entre los objetivos, hipótesis e indicadores.																X				
19. METODOLOGÍA	La estrategia responde a los objetivos de																	X			
20. PERTINENCIA	Es útil y adecuado para la investigación																	X			

II. OPINIÓN DE LA APLICABILIDAD: Existe

III. PROMEDIO DE VALORACIÓN: 82.5 %

Firma del experto informante.

Apellidos y Nombres: MARTINEZ ENRIQUEZ Pedro

DNI N°: 15590438

Anexo Fotografías

Dr. Angel Huaman Tena
ASESOR

M(o). Julio Cesar Valencia Bardales
PRESIDENTE

Ing. Cesar Armando Díaz Valladares
SECRETARIO

M(o). Miguel Angel Aguilar luna Victoria
VOCAL