UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE

FACULTAD DE CIENCIAS E INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

PROPUESTA DE IMPLEMENTACIÓN DE UN HONEYPOT DE SEGURIDAD INFORMÁTICA EN LA AGROPECUARIA WILIAN & ROQUE S.R.L. – CHIMBOTE; 2021.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR

TERRONES BEDON, VICTOR MANUEL

ORCID: 0000-0002-9723-7391

ASESOR

MORE REAÑO, RICARDO EDWIN

ORCID: 0000-0002-6223-4246

CHIMBOTE – PERÚ

2022

EQUIPO DE TRABAJO

AUTOR

Terrones Bedón, Victor Manuel

ORCID: 0000-0002-9723-7391

Universidad Católica Los Ángeles de Chimbote, estudiante de pregrado, Chimbote, Perú

ASESOR

More Reaño, Ricardo Edwin

ORCID: 0000-0002-6223-4246

Universidad Católica Los Ángeles de Chimbote, Facultad de Ciencias e Ingeniería, Escuela Profesional de Ingeniería de Sistemas, Chimbote, Perú

JURADO

Ocaña Velásquez, Jesús Daniel

ORCID: 0000-0002-1671-429X

Castro Curay, José Alberto

ORCID: 0000-0003-0794-2968

Sullón Chinga, Jennifer Denisse

ORCID: 0000-0003-4363-0590

JURADO EVALUADOR DE TESIS Y ASESOR

DR. OCAÑA VELASQUEZ, JESÚS DANIEL

PRESIDENTE

MGTR. CASTRO CURAY, JOSÉ ALBERTO

MIEMBRO

MGTR. SULLÓN CHINGA, JENNIFER DENISSE

MIEMBRO

MGTR. MORE REAÑO, RICARDO EDWIN

ASESOR

DEDICATORIA

A mis padres Marlene y Manuel por siempre apoyarme en mis estudios e incentivarme a siempre a continuar con mis estudios y conseguir mis metas que me planteado. A mi abuelita Sara que siempre está conmigo en los buenos y malos momentos y que nunca me dejará solo, siempre estará para mí y yo para ella.

A Dios ya que sin el nada de esto sería posible realizarlo, por permitir que todo lo cumpla con éxito y que todas mis metas planteadas estoy realizándolas poco a poco.

Victor Manuel Terrones Bedón

AGRADECIMIENTO

En primer lugar, al dueño de la Agropecuaria Wilian & Roque S.R.L don Rolando Guillermo Villanueva Rosales por permitir que mi persona pueda realizar mi investigación dentro de su establecimiento. Además, a las autoridades de la universidad por siempre mejorar la educación que se brinda dentro de la universidad y que cada día vaya mejorando.

También agradecer a mis asesores por orientarme y brindar todas sus enseñanzas para poder culminar con éxito mi investigación que ayudará a culminar mi carrera.

Victor Manuel Terrones Bedón

RESUMEN

La presente tesis fue desarrollada bajo la línea de investigación: Tecnologías de redes de datos e información, de la Escuela Profesional de Ingeniería de sistemas de la Universidad Católica los Ángeles de Chimbote; la problemática es el peligro que existe de ser vulnerado por ataques cibernéticos que quieren robar información de la empresa; tuvo como objetivo: Realizar la propuesta de implementación de un honeypot de seguridad informática en la agropecuaria Wilian & Roque; la investigación fue de tipo cuantitativo y de nivel descriptivo, fue desarrollada con diseño no experimental de corte transversal, mi población fue de 20 personas, entre ellas empleados y clientes y como muestra fue la de las 20 personas; utilice al cuestionario como instrumento de recolección de datos y la encuesta como la técnica, las cuales arrojo los siguientes resultados de acuerdo a mis dimensiones donde; el 65.00% SI creen que es importante la seguridad informática y el 80.00% SI sintieron la necesidad para implementar un honeypot para controlar los ataques cibernéticos; el alcance de estudio es tener un mejor control de los ataques cibernéticos ya que ayuda a conocer los trucos y técnicas que el ciberdelincuente usa para vulnerar el sistema y no verse afectado los clientes y la empresa, concluyendo así que el honeypot fue de gran ayuda para combatir la ciberdelincuencia por ende se vio la necesidad de realizar la propuesta de implementación de un honeypot de seguridad informática con la finalidad de controlar los ataques cibernéticos.

Palabras clave: Ciberataques, Honeypot, Seguridad Informática.

ABSTRACT

This thesis was developed under the research line: Data and information network technologies, from the Professional School of Systems Engineering of the Los Ángeles de Chimbote Catholic University; the problem is the danger of being compromised by cyber attacks that want to steal company information; had as objective: To carry out the proposal for the implementation of a computer security honeypot in the Wilian & Roque farm; the research was quantitative and descriptive level, it was developed with a non-experimental cross-sectional design. My population was 20 people, including employees and clients, and as a sample it was 20 people; I used the questionnaire as a data collection instrument and the survey as the technique, which yielded the following results according to my dimensions where; 65.00% SI believe that computer security is important and 80.00% SI felt the need to implement a honeypot to control cyber attacks; The scope of study is to have a better control of cyber attacks since it helps to know the tricks and techniques that the cybercriminal uses to violate the system and not affect the clients and the company, thus concluding that the honeypot was of great help to To combat cybercrime, therefore, it was necessary to make a proposal to implement a computer security honeypot in order to control cyber attacks.

Keywords: Cyberattacks, Honeypot, Computer Security.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

I. INTRODUCCIÓN

A nivel nacional cualquier situación en la cual suceda algún robo de identidad, accesos no permitidos, daños y perjuicios esos ya se consideran problemas complejos que se necesitan hacer tratados con urgencias y a la brevedad posible; analizando la situación con los virus informáticos que existen en la actualidad, este siempre tratara de hacer daño y perjudicar a todos, tenemos como ejemplo a los robos de información, bloqueo de cuentas del sistema en que el individuo o empresa lo está usando como almacenamiento de su información, saqueo de cuentas bancarias, etc. Estos ataques cibernéticos se pueden prevenir o disminuir para evitar que el intruso ya no robe, con la ayuda de algún software el encargado podría mitigar y evitar estos problemas usándolo como barrera de protección para sus datos (1).

A nivel internacional el honeypot existen para diferentes servicios ya sea de baja o alta interacción, los spammers esperan a que haiga algún desperfecto de la red o con los servidores de correos o proxies que están abiertos para rápidamente los intrusos vulnerar y robar algún dato de la empresa o una persona especifica; se puede crear un honeypots específica para esta situación como lo es SMTP que ayudará a imitar a unos recursos para que se observe a esos ciberdelincuentes que intentan enviar spam. Como lo es el honeynet Project que es una comunidad internacionalmente que se dedica a las investigaciones de estos ataques y a mejorar la seguridad (2).

La problemática de esta sociedad hoy en día es la inseguridad informática que se viene escuchando en todo momento, por lo que la Agropecuaria Wilian & Roque S.R.L. está expuesto a los robos de datos muy sensibles, daños en sus sistemas de ventas, y ya que en la actualidad las cajas fuertes han pasado de moda y todo están guardado en la red ya sea correos corporativos o etc. Porque hay diversidad de técnicas que usan los ciberdelincuentes como los virus troyanos, spam en los correos electrónicos, entre otros virus que se está escuchando hoy en día. Por lo que es más fácil que cualquier hacker pueda robar información que son importantes dentro de la empresa provocando problemas

económicos que causan perdidas por ello la seguridad informática debe ser prioridad para toda empresa.

Por lo que pensaría que este informe podría funcionar para mejorar nuestra seguridad informática en la Agropecuaria Wilian & Roque S.R.L. por ende no nos veamos afectados por personas que desean robar información valiosa de la empresa y tener datos bien seguros y además los datos de los clientes ya que eso es la prioridad de la empresa, por lo que mi enunciado del problema es el siguiente ¿De qué manera la propuesta de implementación de un honeypot de seguridad informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021, mejora el control de los ataques cibernéticos?.

Con la intención de dar solución al problema se planteó como objetivo general: Realizar la propuesta de implementación de un honeypot de seguridad informática en la agropecuaria Wilian & Roque – Chimbote; 2021, con la finalidad de controlar los ataques cibernéticos.

Y como objetivos específicos tenemos los siguientes: Determinar el nivel de importancia de una seguridad informática honeypot en la Agropecuaria Wilian & Roque S.R.L., determinar el nivel de necesidad para implementar un honeypot en la Agropecuaria Wilian & Roque S.R.L., utilizar la metodología PPDIOO de cisco para un correcto trabajo de propuesta de implementación de un honeypot, realizar la simulación de un honeypot de seguridad informática en VirtualBox para controlar los ataques cibernéticos.

El proyecto de investigación se presenta con justificación académico, operativo, económico, tecnológico e institucional; la justificación académica se basa que todo lo aprendido en la universidad nos ayudará a diseñar un honeypot para analizar esos intrusos que deseen robar información a una persona natural o cualquier empresa; la justificación operativa permitirá a la Agropecuaria Wilian & Roque S.R.L. tener la información del intruso o ciberdelincuente que quiere ingresar al sistema gracias al honeypot; la justificación económica beneficiará en la parte monetaria, puesto que gracias al honeypot no habrá perdida económicas que por culpa de ciberdelincuentes se pierden; la justificación

tecnológica seria que el honeypot hace que la red que se encuentra insegura se convierta en la red más segura ya que gracias a esta herramienta se sabrá cuáles son las técnicas que son usadas por los atacantes o ciberdelincuentes y es así que se puede controlar estos ataques; la justificación institucional seria porque los clientes no tendrán ningún miedo o se sientan inseguros de dar sus datos a la empresa, con el honeypot alcanzará una mayor clientela.

Este informe de investigación donde se trabaja con un honeypot de seguridad informática beneficiará bastante a la Agropecuaria Wilian & Roque S.R.L. ya que tendrá como alcance tener un mejor control de los ataques cibernéticos ya que este software ayuda a conocer los trucos y técnicas que el ciberdelincuente usa para vulnerar el sistema.

En el presente informe de investigación su metodología es de tipo descriptivo y de un nivel de investigación cuantitativo de diseño no experimental y de corte transversal.

De acuerdo a mi encuesta realizada obtuve los siguientes resultados de acuerdo a mis dimensiones donde; el 65.00% si creen que es importante la seguridad informática y el 80.00% si sintieron la necesidad para implementar un honeypot para controlar los ataques cibernéticos.

Conforme a los resultados obtenidos, se concluye que es de mucha importancia la implementación del honeypot ya que ayuda para combatir la ciberdelincuencia, por ende, se vio la necesidad de realizar la propuesta de implementación de un honeypot de seguridad informática con la finalidad de controlar los ataques cibernéticos.

II. REVISIÓN DE LA LITERATURA

2.1. Antecedentes

2.1.1. Antecedentes a nivel internacional

Los autores Flores y Quintana (3), en su tesis titulada "Sistema de detección de ataques informáticos a redes de datos empresariales soportado en honeypots" en el año 2018, tuvo como objetivo hacer la implementación del sistema que ayudó al análisis de información sobre los ataques cibernéticos identificando los requisitos, diseñando la arquitectura y realizando las pruebas necesarias para probar la funcionalidad del honeypot, su metodología de esta investigación tuvo carácter de aplicativo pues busca diseñar y desarrollar el sistema, y experimental porque tuvo que comprobar las funciones que tiene el honeypot con casos reales; sus resultados fueron la construcción del sistema si permitió minimizar los ataques y riesgos a la red y sistema; se concluyó que el 66.00% cree que es muy importante el honeypot ya que ayuda al análisis de información sobre los ataques cibernéticos y que se debe procurar eliminar esos ataques identificando las falencias que tiene el mismo sistema; como recomendaciones es tener mejores plugins para distraer y mitigar a los atacantes y no puedan ingresar al sistema.

En el año 2017 el autor Rodríguez (4), en su proyecto de investigación titulada "Estudio de la automatización de una red de sensores global de honeypots", tuvo como objetivos la creación honeynet con base de datos para tener el apoyo de otros usuarios, estudiar honeypot lo más actual para incorporar honeynet, hacer la simulación para comprobar honeypots, analizar esos ataques y ocultar al honeypots para los atacantes visualizando datos rápidamente; su metodología son de tipo descriptivo y de un nivel cuantitativo, como resultados tenemos que la creación de máquina virtual si ayuda a la agregación de otros sensores para comprobar su

eficacia en la red; se concluyó que el honeypot es muy valioso y tiene un gran potencial en seguridad informática para trabajar en detectar con sistemas falsos y poder visualizar los ataques y hacer un análisis de forma muy rápida, las recomendaciones es hacer un sistema para que el usuario registre todos los datos recogidos por la máquina virtual.

El autor Matus (5), en el año 2017 en su trabajo de tesis titula "Análisis e implementación de una solución honeypot para un entorno experimental"; su objetivo de esta investigación fue configurar e implementar las diferentes soluciones de un honeypot en Linux con riesgos experimentales, hacer las instalaciones y configuraciones para emplear en una cama de pruebas, realizando ataques para ver si funciona correctamente las funciones que este honeypot tiene; su metodología es experimental porque va a necesitar varias instalaciones, configuraciones e cada uno de los honeypot que se trabajará; sus resultados obtenidos son que los tres software que se trabajó para esta investigación tiene una diferente finalidad con interfaces graficas que se tuvieron que evaluar; se concluyó que el 90.00% estuvo de acuerdo que haga la implementación del honeypot ya que es muy necesario, y el 10.00% no y que la seguridad en los sistemas de información son muy importantes en toda clase de empresa para tener confidencialidad y salvaguardar la información; como recomendaciones es utilizar archivos para registrar esos datos que el honeypot genera o almacenarlo en alguna base de datos.

2.1.2. Antecedentes a nivel nacional

El autor Ochoa (6), en su tesis titulada " Diseño de una red de seguridad informática para la protección del sistema web de un call center ante ataques informáticos aplicando la norma iso 27033" en el año 2019; su objetivo fue hacer el diseño de la red con requisitos de la iso 27033 que ayuda a tomar acciones para que se proteja al

sistema web de call center; la metodología lo clasificaron en la escala cuantitativa y cualitativa porque tendrá un impacto con su objetivo de la empresa elaborando así su matriz de riesgos que esta puede correr mediante la investigación; sus resultados fueron que el 41% de la información son de nivel críticos ya que esto perjudica al call center poniendo en riesgo toda su información, por lo que el sistema web debe ser atendido a la brevedad para no ser vulnerados y poner en riesgo al cliente y la empresa; se concluyó que se llegó a identificar los riesgos en la que está expuesta la empresa call center por lo que la norma 27033 ayuda a obtenerlo para otorgar el control necesario para estos ataques; se recomendó revisar bien las normas iso 27001 por el motivo de tener al alcance los tratamientos de riesgos de ataques.

En el año 2018 el autor Romero (7), con su tesis titulada "Propuesta de seguridad informática para mejorar el proceso de acceso remoto en entidad financiera", su objetivo fue dar un solución sobre seguridad informática para mejorar los procesos de la entidad financiera, además ver cual el nivel de conocimiento y riesgo para proponer una adecuada seguridad informática en la empresa, su metodología es con un enfoque cuantitativo y no experimental puesto que no se modifica la variable de estudio, además es de tipo correlacional; sus resultados fueron que gracias a la propuesta del proceso este mejorara la seguridad informática teniendo así un nivel de conocimientos más altos para poder hacer la practica a algunos de los empleados, autenticando los datos reduciendo así los riesgos de ataque; se concluyó que los trabajadores no tenían mucho conocimiento acerca de la seguridad informática y cómo reaccionar ante cualquier eventualidad ya que nadie estaba capacitado para esta situación; las recomendaciones es que la financiera realice varias capacitaciones a los empleados para que cada día ellos ya estén bien preparados para cualquier ataque.

El autor Pomalaya (8), en el año 2018 según su tesis de investigación titulada "Rediseño de la red de datos para mejorar la seguridad informática de una municipalidad", tuvo como objetivo rediseñar una red mejorando la seguridad de la municipalidad estableciendo la manera de integrar el rediseño de los datos; su metodología fue de nivel descriptivo – explicativo, y de diseño pre experimental con el enfoque cuantitativo puesto que habrá una manipulación de la variable independiente para ver sus efectos a la variable dependiente; sus resultados obtenidos fueron que hubo una disminución de pérdidas en paquetes de transmisión de datos en un 7.53% en la municipalidad; se concluyó que tuvo una disminución del 92.8% a los accesos en los servicios no autorizados con el pre test y el post test que se usó en el proyecto; se recomendó implementar el rediseño porque gracias este se optimizo la confidencialidad, integridad y disponibilidad de la empresa investigada.

2.1.3. Antecedentes a nivel regional

El autor Llerena (9), en su tesis titulada "Evaluación de la seguridad informática en el área de sistema de la municipalidad distrital de nuevo Chimbote" en el año 2018; sus objetivos es evaluar los tipos de vulnerabilidades para poder tomar medidas para mejorarlo en el área de sistemas de la empresa; su metodología es documental – descriptiva para recolectar los datos para hacer el estudio necesario y de diseño no experimental y de corte transversal puesto que al recolectar los datos será en un solo momento; sus resultados fueron que el personal no tiene el apoyo de la dirección encargada y también no tiene un seguimiento continuo en sus procedimientos y políticas; se concluyó elaborando un plan de estrategia para así mejorar los procesos de importancia en el área de sistemas en que se debe tomar conciencia de esto; se recomendó mejorar los procedimientos en el que la área de sistemas maneja adecuando la gestión y seguridad como normas de calidad.

En el año 2017 el autor De La Cruz (10), según la tesis titulada "Aplicación de metodologías y herramientas de la informática forense para reducir el riesgo de la seguridad informática en la dirección nacional de comunicación y criminalística de la policía nacional del Perú – Huaraz – 2015", tuvo como objetivo hacer la relación que existe la informática forense y seguridad informática en la PNP conociendo las características los niveles de estas dos relaciones; su metodología es de carácter aplicado, de alcance transversal y con un nivel relacional y descriptiva y de diseño no experimental; su resultado fue que es muy importante conocer la seguridad informática para que se puedan desempeñar en la función de ayudar a la aplicación, se concluyó que se debe mejorar los fortalecimientos de las capacidades en informática forense a la PNP; se recomendó que creen capacitaciones para que fortalezcan el nivel de capacidad en informática forense.

El autor Alvarado (11), en su tesis titulada "Análisis de las vulnerabilidades mediante el uso de phishing para mejorar la seguridad informática de los equipos de cómputo y redes de la municipalidad distrital de independencia" en el año 2017, su objetivo fue la aplicación de ciertas técnicas para analizar vulnerabilidades a través de phishing para la municipalidad investigada, y alertar los riesgos que se corre a través de la internet por lo que se debió hacer la creación de un caso práctico de cómo manejar la situación ante un riesgo o ataque cibernéticos; su metodología es no experimental y de estudio exploratorio y descriptivo; sus resultados fueron que los riesgos de amenazas podrían paralizar todas las actividades por lo que es incalculable las perdidas en la empresa; se concluyó que la municipalidad podría contar con mejores tecnologías de equipos y software de seguridad para mitigar los riesgos y perdidas por el ataque de phishing, se recomendó crear conciencia y capacitar a los empleados sin importar su área de trabajo ya que todos deben estar preparados para cualquier situación.

2.2. Bases teóricas

2.2.1. Rubro de la empresa

La empresa investigada Agropecuaria Wilian & Roque S.R.L. en la actualidad está contando con una tienda principal en la ciudad de Chimbote, que se ubica en Jr. Francisco Pizarro Nro. 859 P.J. el Progreso y una sucursal en Av. José Gálvez Nro. 768 P.J. el Progreso – Chimbote. La agropecuaria mantiene un sistema de ventas donde se caracteriza por vender variedades de productos agrícolas para los cultivos en el campo como, por ejemplo: Abono, urea, sulfato de amonio, nitrato de amonio, cloruro de potasio, fosfato de amonio, insecticidas, fungicidas, herbicidas, también ofrece bombas de mano para la fumigación en el campo, entre otros productos, además se dedica a dar asesoramiento a los agricultores de cómo mejorar los cultivos, y darles a conocer los nuevos productos que salen a la venta para terminar con plagas de sus sembríos (12).

2.2.2. La empresa investigada

En la Agropecuaria Wilian & Roque S.R.L., las tiendas están enfocadas a distribuir y ofrecer productos a los campesinos y agricultores que necesitan de sus productos para sus cultivos en el campo. Su público es mayormente gente adulta que busca terminar con plagas en sus siembras y además gente que quiere mejorar sus cultivos mediante fertilizantes que ayudan bastante a las plantas a su crecimiento y mayor producción de esta, además esta empresa se encarga de mandar información a personas que quieran participar en su asesoramiento de cultivos. También esta empresa manda la información de todo el stock, precios e información que requiere la tienda sucursal que esta dispone (12).

- **Información general**

RUC: 20600381751

Razón Social: AGROPECUARIA WILIAN & ROQUE S.R.L.

Nombre Comercial: Agrícola Serrano.

Fecha de inicio de actividades: 27/10/2007

Gerente General: Rolando Guillermo Villanueva Rosales

Dirección: Jr. Francisco Pizarro Nro. 859 P.J. el Progreso

Dirección: Av. José Gálvez Nro. 768 P.J. Progreso

Distrito / Ciudad: Chimbote

Provincia: Santa

Departamento: Ancash, Perú

- **Ubicación**

Gráfico Nro. 1: Ubicación de la agropecuaria Wilian & Roque S.R.L.

Fuente: Google Maps (13).

- **Historia**

EL señor Rolando Guillermo Villanueva Rosales, decidió construir su negocio dedicado a la comercialización de Insumos para el uso Agrícolas dirigido a la venta en la provincia del Santa en el año 2007 por tal motivo en la fecha 27 de octubre del año mencionado se inscribió en la Sunat de la ciudad de Chimbote iniciándose como único punto de venta en el P.J. El progreso Nro. 859 Jr. Francisco Pizarro, con el pasar de los años, en el 2015 vio la oportunidad de abrir una sucursal, pero ya con una razón social de Agropecuaria Wilian & Roque S.R.L. decidió abrir esa tienda ya que en ese momento había mucha demanda de productos en el sector agrícola y es así que posteriormente apertura el establecimiento sucursal como punto de venta, ubicado en el P.J. Progreso – Av. José Gálvez Nro. 768, y con la visión de apertura en próximos puntos de venta en otras ciudades (12).

- **Objetivos organizacionales**

  - **Visión**

    "Comercializar los productos a nivel departamental y regional estableciendo punto de venta y sucursales en diversos distritos de la región".

  - **Misión**

    "Prestar el mejor servicio y asesoramiento técnico además de los mejores productos y de calidad garantizada. Para así poder llegar a cubrir la expectativa de los agricultores".

- **Funciones**

Administrador

- Recepcionar documentos del personal nuevo.
- Mantener actualizado el archivo documentario.
- Toma de decisiones en la empresa.
- Interviene en tareas de consultoría y la administración del personal en tareas de búsqueda y evaluación.
- Elaboración de contratos para trabajadores.
- Entrega de liquidaciones al personal.

Contador

- Controla la contabilidad de la empresa.
- Interviene en los documentos de cobro y pagos correspondientes.
- Formular el presupuesto, gastos, ingresos y cuentas generales con el administrador.
- Encargado de estados financieros y los análisis.
- Certificación de planillas por pagos de impuestos.

Secretaria

- Gestionar documentos.
- Recibir y ordena documentos.
- Enviar y recepcionar correos electrónicos.
- Manejar la información.
- Llena todas las facturas.

Vendedor

- Conocer el producto.
- Atención al cliente.
- Vender los productos.
- Fidelizar al cliente.

- **Organigrama de la empresa**

Gráfico Nro. 2: Organigrama de la Agrícola Serrano.

Fuente: Elaboración propia.

- **Infraestructura tecnológica**

Agropecuaria Wilian & Roque S.R.L. actualmente cuenta con 5 computadoras Intel Core i3, de 4gb de RAM y 500gb de almacenamiento. Además, impresora de la marca Epson modelo 1460 que sirve para la impresión de los comprobantes de pago; y por último un router que distribuye internet a toda la empresa agrícola.

2.2.3. Las tecnologías de la información y comunicaciones (TIC)

Es un conjunto de herramientas, aplicaciones, almacenamientos, programas, que nos permite compilar, datos, textos, imágenes entre otras. Las tics tiene que ser usados de manera muy apropiada para desarrollar una sociedad con democracia que nos fortalecerán la creatividad, colaborar que ayude a una colaboración más equitativa (14).

Para tener una mayor formación y aprendizaje en los tics deben tener una facilidad en contar con internet. En la era de la comunicación y la información, se considera que el aprendizaje será la base para el desarrollo, el crecimiento y el progreso de la sociedad. Por lo tanto, el sistema educativo debe favorecer la formación continua y permanente de los docentes en cada uno de los niveles educativos, a fin de responder a las necesidades, los intereses y los retos de la población estudiantil (15).

Su historia de las tecnologías de información y comunicación comenzó en la época moderna con la década de los 70 al comenzar con la revolución digital. Por lo que las búsquedas de diferentes herramientas para que se puedan comunicar con personas que están en otros países o a cierta distancia por lo que se creó el teléfono algo muy fundamental en la actualidad (15).

El salto que ayudo a elevarse las tecnologías de información y comunicación fue las computadoras que se creó con el paso de los años, se fueron mejorando los modelos y con diferentes y podían ser más asequibles y la gente lo usaban más (16).

Ya en la década de los 80 aparecieron los diferentes modelos de celulares móviles con menos tamaño y con un mejor precio para que la población pueda adquirir uno de estos móviles. En la década de

los 90 hasta la actualidad las computadoras y celulares van mejorando sus capacidades y tienen mejores técnicas para usar. Ya que la internet hoy en día es algo que casi toda la población cuenta con teléfono móvil que está al día con toda la globalización. Esto de la internet fue mejorando más y más por lo que la velocidad y calidad de transmitir los datos cada día se van mejorando y se seguirá haciendo porque es muy importante para la población (16).

- **Las TIC más utilizadas en la empresa investigada**

Las tics en la que la agropecuaria usa son correos electrónicos en la que envían datos a sus clientes por ejemplo una boleta electrónica, además usa un sistema para registrar todas las ventas diarias de todos los clientes, también de llevar el control e inventario de todos los productos a la hora de recibir toda la mercadería (16).

2.2.4. Teoría relacionada con la Tecnología de la investigación

2.2.4.1. Ataques Cibernéticos

Es una serie de riesgos que llevan al navegar por la internet usando las tecnologías de información y comunicación frente a los ciberdelincuentes que están ahí para actuar al acto delictivo. Cuando escuchamos delitos o ataques cibernéticos decimos los hackers, ya que están son peligrosos afectando sistemas, secretos informáticos, entre otros aspectos (17).

2.2.4.2. Seguridad Informática

Es un conjunto de métodos, normas, técnicas, procedimientos que ayudan a regular el diseño, desarrollo, sobre las tecnologías de información y comunicación que hace que el sistema sea confiable y bastante seguro. Se debe

reaccionar ante cualquier situación de riesgos generales o específicos de manera urgente (18).

2.2.4.3. Honeypot

El honeypot va a consistir en que esta herramienta crea una seguridad informática dentro en nuestra red como objetivo de atrapar y engañar con un señuelo, de esta manera los ataques que son externos se dirijan en él y no en archivos importantes de tu negocio. Se puede engañar a los ciberdelincuentes mediante software específico creado por especialistas, o bien a través de la acción humana directa. La base de crear un buen honeypot es simular que la empresa que quiere implantar este sistema genere puertas de entrada a sus sistemas, haciendo parecer de cara al exterior que la empresa está poco protegida, o directamente "a verlas venir" (19).

- **Historia**

Una de las primeras historias de alto perfil de Infosec involucró lo que seguramente fue el primer uso de un honeypot. Como se detalla en su libro, The Cuckoo's Egg, en 1986, Clifford Stoll, administrador del sistema de la Universidad de Berkeley, intentó rastrear un cargo aparentemente erróneo de 75 centavos de dólar por el uso de un sistema Unix en Lawrence Berkeley Lab. En el proceso, descubrió que alguien estaba ingresando al sistema y había logrado obtener acceso de superusuario. Stoll implementó dos defensas tipo honeypot para rastrear al hacker: conectó terminales prestados a las cincuenta líneas telefónicas entrantes durante un largo fin de semana y esperó a que el hacker llamara; al darse cuenta de que el

atacante estaba buscando información sobre los secretos de la defensa nuclear, creó un departamento completamente ficticio en LBL que supuestamente trabajaba en el sistema de defensa de misiles «Star Wars» para atraer al hacker a pasar tiempo ahí. Finalmente, el atacante fue arrestado y se reveló que era un alemán occidental que trabajaba para la KGB (20).

Otro importante incidente temprano de honeypot se produjo en 1990, cuando un hacker intentó ingresar a AT&T Bell Labs y robar su archivo de contraseñas. El pionero de Internet, Bill Cheswick, que trabajaba para Bell Labs en ese momento, dirigió al atacante hacia lo que llamó «una persecución alegre» a través de algunos sistemas ad hoc de honeypot para rastrear su ubicación y aprender sus técnicas. Su escrito del incidente, «An Evening with Berferd» fue extremadamente influyente (21).

Pronto, los honeypots comenzaron a convertirse en una parte más estandarizada de la caja de herramientas del profesional de seguridad. El proyecto Deception Toolkit se lanzó en 1997; aunque ahora está inactivo, su sitio web aún está en funcionamiento con el glorioso diseño de finales de los años 90. El Proyecto Honeynet, que comenzó en 1999, sigue activo hoy como un recurso de la comunidad de seguridad (20).

- **Tipos de honeypots.**

En este sentido cobra importancia el grado de interactividad que se tenga con el atacante, diferenciando entre los honeypots de baja interacción y los de alta interacción. En

los honeypots de baja interacción la imitación de sistemas o aplicaciones reales es el punto más fuerte, simulando funciones solamente en la medida que sea posible que se produzca un ataque. En los de alta interacción se implementan sistemas reales que ofrecen los servicios de un servidor, de ahí que se tengan que supervisar y proteger correctamente, con los riesgos que toda la operación conlleva (20).

- **Funciones**

Por entrar en algo de detalle, un honeypot funciona así: Para

saber acerca más de los posibles ataques cibernéticos
se debe tomar una partida y hacer una serie de servidores o ciertos sistemas para que parezca algo sensible o fácil de que algún intruso quiera intentar robar los datos. Este trabajo necesita bastante tiempo y esfuerzo porque en el camino se puede encontrar con momentos vulnerables que hacen que te flaquees y quieras cerrar las tareas de seguridad (19).

En el momento que toda la trampa se haya puesto en su lugar, este se debe de poner algún dato importante para que el atacante caiga rápidamente pensando que la empresa esta vulnerable con sus datos de alguna empresa o algún individuo. Pero lo que en realidad el hackers está haciendo es entrar a la zona de seguridad que está siendo protegida y bien seguro, rastreando todos los movimientos que hace el atacante, cortándole el acceso a que ya no pueda ingresar al sistema (19).

Los diferentes beneficios en el que se basa los que trabajan con algún software para contener los ataques cibernéticos es dar posibles ataques reales con información muy valiosa para que supuestamente el intruso quiera robar esa información y asiendo que el atacante se maree en lo que hace ya que está bien seguro y así intente las diferentes formas por ingresar este no podrá y así la persona de seguridad informática analizara todos los movimientos que haga durante el intento de querer entrar al sistema (19).

- **Otras soluciones utilizadas para crear honeypots**

Hace muchos años, en el mercado existen herramientas importantes que pueden servir para adentrarse en este campo, teniendo en cuenta que ya deben estar previstas por los atacantes. Algunas de ellas son:

Honeyd: Fue creada por Niels Provos y, aunque es un solo honey pot en GNU/Linux o Windows, el atacante verá múltiples servidores panales. Honeyd crea diferentes direcciones IP virtuales, cada una con los puertos y servicios que deseemos emular. Para ayudar a comprender el concepto, imaginemos un aparato enrutador conectado por un módem a Internet y con un disco duro conectado con varias máquinas virtuales corriendo, cada una con diferentes puertos y servicios abiertos (22).

HoneyBOT: Fue creada para Microsoft Windows y tiene una interfaz gráfica integrada, por lo que conviene en elegirla cuando una persona está entrando en el mundo de los honeypots. Su característica es el nivel de lo que guarda ya que almacena en byte y con una gráfica excelente para

tener una mejor visualización. Es un software privado y pertenece a “Atomic Software Solutions” (23).

Specter: Este es más poderoso, ya que cuenta con perfiles pre configurados de diferentes sistemas operativos, además hace la inyección de datos codificados al atacante para luego ser usados como prueba. Abre perfiles personalizados y acumulativos de cada intruso. Este software no necesita de ninguna manipulación o monitoreo ya que este viene predefinido con diferentes datos que están a salvo con código cerrado (24).

Kippo: Este programa escrito en Python y se aloja en GitHub con una licencia libre. Se conoce como un honeypot de interacción mediana, una categoría intermedia a las que describimos previamente, ya que se enfoca en SSH (24).

Honeynets: Es un tipo especial de honeypots de alta iteración que se puede estar en plataformas como Windows, Linux entre otras. Esto permitirá capturar toda la información parecido a las soluciones de un honeypot, pero más complejo, ya que se necesita de implantación, la administración y el monitoreo constante para prevenir riesgos (25).

- **Ubicación**

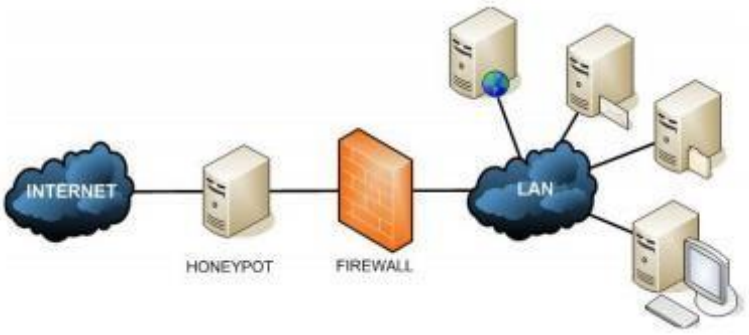
Cuando se menciona a un honeypot, se debe tener mucho en cuenta cual será el lugar donde se implementará dentro de la empresa, ya que se debe considerar la ubicación dentro de la red en la cual este honeypot hará el trabajo. Para la ubicación de este se tomará mucho encuentra las ventajas y

desventajas que tiene para obtener mayores resultados y tener una efectividad y una mayor cantidad de números de ataques que ayuden mucho a mi investigación. Por ello estas son las siguientes ubicaciones de honeypot:

- **Honeypot antes del Firewall**

  En esta ubicación posicionada un honeypot se encuentra directamente con el intruso o ciberdelincuente por ello este ayuda a tener un número mayor de registro de ataques que quieren perjudicar a nuestro sistema siendo esto filtrada por el firewall y no verse afectada nuestra red interna por ningún ataque. Esta ubicación ayuda a que se tenga una estadística real sobre estas eventualidades de ataques que quieren robarnos información; pero como desventaja de esta ubicación es que solo captura ataques externos mas no los ataques internos que puede sufrir nuestra red (26).

Gráfico Nro. 3: Honeypot antes del firewall



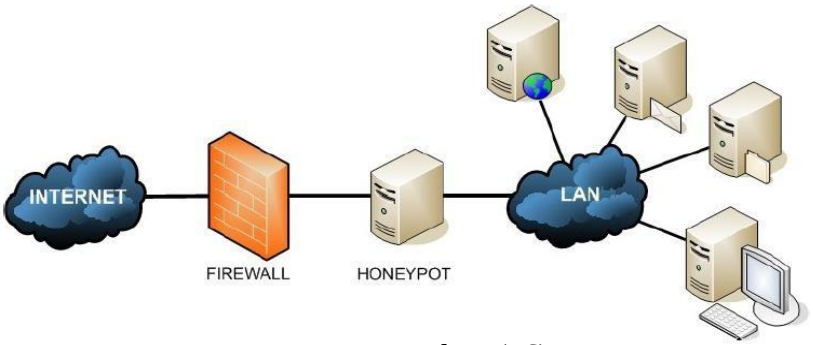
Fuente: Verdejo (26).

- **Honeypot después del Firewall**

  En esta ubicación de honeypot tiene una gran ventaja lo cual es hacer la recopilación de todos los ataques internos dentro de la red, y además de se puede blindar

nuestro firewall ya que se detectaría si la configuración del firewall está teniendo problemas y por ende se debe hacer la creación de nuevas reglas de filtraciones para el firewall. Pero como desventaja de esta ubicación es que no se puede hacer la recopilación de mucha información como la ubicación que se tiene delante del firewall (26).

Gráfico Nro. 4: Honeypot después del firewall

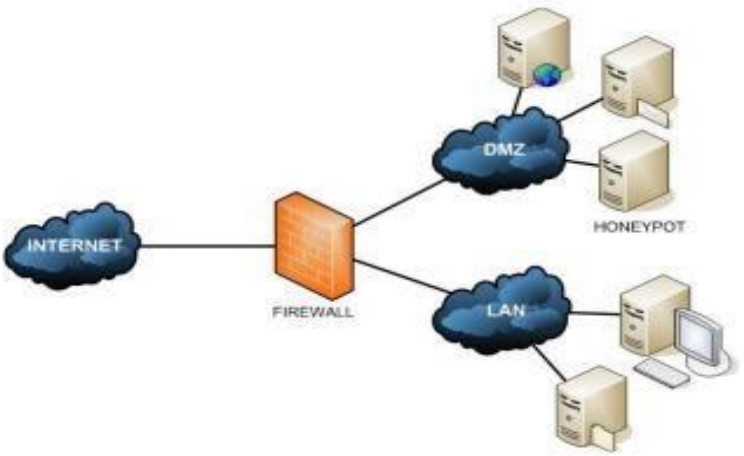


Fuente*:* Verdejo (26).

- **Honeypot en una DMZ**

También se le puede llamar zona desmilitarizada (Demilitarized zone), en esta ubicación el honeypot se encuentra entre la red interna y externa que generalmente en la internet, siendo así de gran ayuda configurando en el firewall. Si este honeypot se ubica en este lugar se evita si hay la existencia de un IDS que está configurado en la red de las alertas que se generan en el tráfico del honeypot ya que no afecta al IDS, ya que esta ubicación del honeypot en la zona desmilitarizada se encuentra fuera del alcance de IDS. Pero como desventaja en esto es que se tiene algunas pérdidas de tráficos de ataques internas, ya que para poder acceder al honeypot se tiene que hacer esto de una forma explícita (26).

Gráfico Nro. 5: Honeypot en una DMZ



Fuente: Verdejo (26).

2.2.4.4. Firewall

También se le puede llamar cortafuegos que es un sistema de seguridad de red que se encarga de proteger la maquina o la subred de los servicios exteriores que pueden ser amenazas. El firewall también se explica como el filtro ya que examina cada paquete de información mediante la política de seguridad para aceptar, modificar o bloquear cualquier dato (27).

2.2.4.5. Base de datos

MySQL

Este es un sistema de bases de los datos relacionales con una licencia de software libre ya que esta puede ser copiada y adaptada como el usuario quiera hacerlo; además es fácil de adquirirlo. Desde el 2000 su licencia está bajo GPL (GNU Public Licence) La información de esta base de datos está compuesta por tablas, registros, y columnas. Trabaja con una arquitectura cliente/servidor que permite que

trabaje con multiusuarios, es decir, establece conexiones con el servidor creando subprocesos para autorizar las solicitudes del cliente. Es bastante ideal para trabajar con accesos de páginas webs muy dinámicas, que implica guardar información, y realizar múltiples consultas (28).

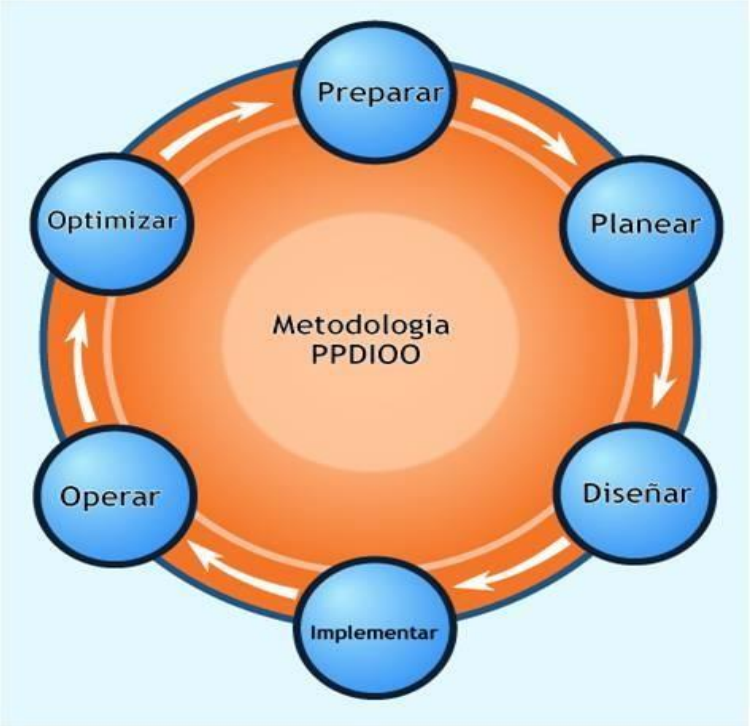
2.2.4.6. VirtualBox

Este es un software que virtualiza sistemas operativos, que ayuda a crear sistemas operativos dentro de un sistema operativo. Además, deja cambiar el sistema operativo de la maquina a otra, simplemente con pasar de una ventana a otra sin tener ninguna complicación. Brinda la opción de no hacer ninguna modificación en tu computadora ya que será una maquina independiente con entorno seguro. Su licencia es gratuita y de Oracle VM para usarlo como prueba o personal, por ende es fácil de adquirirlo simplemente descargándolo en su página web oficial (29).

2.2.5.7. Metodología PPDIOO

Esta posee alineamientos que van del ciclo de vida del ppdioo que se usa por Cisco con el fin de administrar una red. Este ciclo de vida es bastante útil para lograr una implementación de otras nuevas redes, como para actualizaciones de existentes redes. Están formadas por elementos en forma de círculos que conllevan a realizar actividades para lograr cambios y validar toda la infraestructura que se tiene, empezando por el primer paso que es preparación, planeación, diseño, implementación, operativa y culmina con la optimización (30).

Gráfico Nro. 6: Metodología Ppdioo



Fuente: Lagla (30).

Beneficios

- Ayuda a disminuir los costos para realizar las validaciones de los requerimientos como de: tecnología, planeación, infraestructura y recursos. Esto conlleva a alinear los requisitos técnicos y tener claro los objetivos de la empresa. Y asi mejorar la red y disminuyendo los costos de los operativos (30).

- Se aumenta la posibilidad de que la red proporcione un diseño solido considerando una alta seguridad de un diseño propuesto. Por ello se podría ejecutar pruebas pilotos o quizás prototipos que llevarían a la implementación de la red (30).

- Agilizar los requisitos de negocio, técnicos y los objetivos que están diseñados con alto dominio de configuraciones, instalación y la integración de todos los componentes del sistema que existen para una mejora continua (30).

- Ayuda a tener una mejor velocidad de las aplicaciones y los servicios para un análisis profundo de todos los objetivos, análisis, y tecnologías que pueden ser implementadas soportando servicios de red y además de aumentar la disponibilidad de la red (30).

Fases del ciclo de vida del PPDIOO

Entre ellas tenemos (30):

- Fase de la preparación: En esta fase se encarga de ver todo el presupuesto y las estrategias de red.

- Fase de la planeación: En esta fase se involucra las evaluaciones de la red y realizar los análisis correspondientes de las deficiencias.

- Fase del diseño: En esta fase se encarga de diseñar la solución es decir el producto que se está trabajando o los servicios.

- Fase de la implementación: En esta fase se pone en marcha las soluciones que se planteó dentro de la fase 2.

- Fase operativa: En esta fase se realiza el mantenimiento de la red que se planteó e instalo anteriormente.

- Fase de optimización: En esta fase se encarga la administración de la red.

2.2.5.8. Metodología Top-down Network Desing

Esto es una metodología que cuenta con 4 fases que ayudan para el diseño de redes, entre estas son las siguientes:

La fase de análisis de negocios objetivos y limitaciones: En esta se identifica los objetivos y todas las restricciones de la empresa, como también las caracterizaciones de la red existente y todo lo que tiene que ver con el tráfico de la red. De esta manera se llegará a conocer la línea de la empresa y cuál es su estructura organizacional, se logra determinar las autoridades que estarán responsables para que se acepte el nuevo diseño de red, y como último punto se identifica todos los cambios que se proyecta generar (31).

La fase de diseño lógico: Se logra diseñar lo que viene hacer la topología de red, además del modelo de nombramiento y del direccionamiento, se lograra seleccionar los protocolos de switching, routing y bridging para la interconexión. También esta fase incluye toda la seguridad y lo que es la administración de la red (31).

La fase de diseño físico: En esta se seleccionará las nuevas tecnologías y todos los dispositivos que se requirieron técnicamente por la fase anterior del diseño lógico (31).

La fase de pruebas, optimización y documentación de la red: Se empieza con usar las pruebas que se logró construir como prototipo para las pruebas, además de la prueba que se debe introducir en su análisis del tiempo de respuesta, rendimiento, disponibilidad y la regresión. También en esta fase se optimiza el uso de acho de banda y además como ultimo la documentación de todos los contenidos del nuevo deseño de la red (31).

III. HIPÓTESIS

3.1. Hipótesis general

La propuesta de implementación de un honeypot de seguridad informática en la agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021, permitirá controlar los ataques cibernéticos.

3.2. Hipótesis específicas

1. La determinación del nivel de importancia de una seguridad informática honeypot permitirá tener un mejor punto de vista para la realización del proyecto de investigación.

2. La determinación del nivel de necesidad para implementar permitirá ver si es necesario o no la implementación del honeypot dentro de la agropecuaria Wilian & Roque S.R.L.

3. La utilización de la metodología PPDIOO de cisco permitirá trabajar de forma correcta nuestra investigación.

4. La realización de la simulación de un honeypot de seguridad informática en el VirtualBox permitirá tener una mejor opinión de lo que conviene trabajar con el honeypot.

IV. METODOLOGÍA

4.1. Tipo de la investigación

Cuantitativo: Se refiere que este se encarga de la recolección de todos los datos que probaremos con las hipótesis planteadas haciendo una medida numérica y un análisis estadístico con la finalidad de probar las teorías planteadas. Las decisiones que se toman para recolectar la información están estructuradas y que serán representado por la población. Al finalizar el estudio cuantitativo se desea confirmar y anunciar todos los fenómenos que se investiga, hallando relaciones y regularidades en la investigación de estudio (32).

4.2. Nivel de la investigación

Descriptiva: El nivel de investigación descriptiva ayuda a especificar todas las propiedades y las más importantes características de la variable de estudio en la que se trabajando. Este pretende medir y recoger la información para describir situaciones y sucesos recogidos en un grupo, comunidad o una población especifica. La descripción puede ser profunda o no tanto, pero de igual manera este nivel de investigación se basa en hacer la medición de una o varias variables (32).

4.3. Diseño de la investigación

El diseño de la investigación será no experimental ya que no se creó ninguna muestra para el estudio, y por las características de la su ejecución será de corte transversal.

No experimental: Es el estudio que se hace sin manipular las variables deliberadamente y que solo se observa los fenómenos para poder analizarlos en el proyecto de investigación (32).

Transversal: Esto se refiere a que la información recolectada se hace en un solo momento y se encarga de describir y analizar las variables de investigación (33).

El esquema del diseño de la investigación tendrá la siguiente estructura:

Dónde:

M = Muestra

O = Observación

4.4. Población y muestra

Población

En esta investigación el universo en la agropecuaria Wilian & Roque es de 3 trabajadores, pero por lo que es número menor que necesitamos para nuestra investigación, trabajaremos en conjunto con los clientes para tener unos mejores resultados en el proyecto de investigación.

Población: Se refiere al total de un fenómeno de la cual se está estudiando, ya sea personas, objetos que está cuantificado en un conjunto N de entidades que participan en el estudio (34).

Muestra

Como muestra de la investigación se seleccionó a los 3 trabajadores de la empresa agropecuaria Wilian & Roque y a 17 clientes más recurrentes, no se utilizó ninguna fórmula estadística, se hizo por conveniencia.

Muestra: Esto es una cierta cantidad de la totalidad de la población que se cuantificó en la población de la cual se está estudiando en el proyecto de investigación, que sirve para representarlo puesto que hay situaciones donde la población es muy extensa (34).

4.5. Definición de operacionalización de variables e indicadores

Tabla Nro. 1: Operacionalización de las variables

Variable	Definición Conceptual	Dimensiones	Indicadores	Escala medición	Definición Operacional
Honeypot de seguridad informática para controlar ataques cibernéticos	Honeypot: Esta herramienta crea una seguridad informática dentro en nuestra red como objetivo de atrapar y engañar con un señuelo, de esta manera los ataques que son externos se dirijan en él y no en archivos importantes de tu negocio.(19). Ataques Cibernéticos: Es intentar, perjudicar o querer dañar un sistema informático o de una red mediante virus que dañan o eliminan datos de quipos o programas (35).	Nivel de Importancia de una Seguridad Informática Honeypot.	- Software de seguridad. - Herramientas honeypot. - Vulnerabilidad de sistemas. - Ataque cibernético. - Análisis de honeypot.	Ordinal	Es una herramienta que se ejecuta mediante comandos que ayuda a la empresa Agropecuaria Wilian & Roque S.R.L. a engañar a los ciberdelincuentes que quieran robar información.
		Nivel de necesidad para implementar un honeypot.	- Beneficio de implementación. - Estabilidad y seguridad. - Perdida de información. - Pérdidas económicas. - Seguridad de información.		

Fuente: Elaboración Propia

4.6. Técnicas de instrumentos de recolección de datos

En esta investigación se usó la técnica de la encuesta y la recolección de datos mediante el cuestionario.

Encuesta: Es una técnica para recoger datos a través de interrogaciones con la finalidad de obtener conceptos claros que derivan la problemática del proyecto de investigación (36).

Cuestionario: Es el instrumento para recoger los datos donde están todas las preguntas formuladas y bien ordenadas, para así poder recolectar la información rápidamente a la muestra que se desea hacer (36).

Se seleccionará a las personas adecuadas, para poder aplicar los cuestionarios, ya que así obtendremos la información apropiada, por medio de visitas a la instalación de la Agropecuaria Wilian & Roque S.R.L.

Asimismo, se entregará los cuestionarios a las personas seleccionadas, para poder resolver cualquier duda en relación a las interrogantes planteadas en los mismos.

Se creará un archivo en formato MS Excel 2016 para la tabulación de las respuestas de cada cuestionario en base a cada dimensión de estudio, así se obtendrá rápidamente los resultados y se podrá dar su conclusión a cada una de ellas.

4.7. Plan de análisis de datos

Recolectada la información con las técnicas y procedimientos mencionados anteriormente, se creará una base de datos temporal en el software Microsoft Excel 2019, y se procederá a la tabulación de los mismos. Se realizará el análisis de datos con cada una de las preguntas establecidas dentro del cuestionario dado permitiendo así resumir los datos
en un gráfico que muestra el impacto porcentual de las mismas.

4.8. Matriz de consistencia

Tabla Nro. 2: Matriz de consistencia

<table>
<tr><td>Problema</td><td>Objetivo general</td><td>Hipótesis general</td><td>Metodología</td></tr>
<tr><td rowspan="3">¿De qué manera la propuesta de implementación de un honeypot de seguridad informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021, mejora el control de los ataques cibernéticos?</td><td>Realizar la propuesta de implementación de un honeypot de seguridad informática en la agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021, con la finalidad de controlar los ataques cibernéticos.</td><td>La propuesta de implementación de un honeypot de seguridad informática en la agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021, permitirá controlar los ataques cibernéticos.</td><td rowspan="3">Tipo: Cuantitativa

Nivel: Descriptiva

Diseño: No experimental y de corte transversal</td></tr>
<tr><td>Objetivos específicos</td><td>Hipótesis específicas</td></tr>
<tr><td>1. Determinar el nivel de importancia de una seguridad informática honeypot en la agropecuaria Wilian & Roque S.R.L.

2. Determinar el nivel de necesidad para implementar un honeypot en la agropecuaria Wilian & Roque S.R.L.</td><td>1. La determinación del nivel de importancia de una seguridad informática honeypot permitirá tener un mejor punto de vista para la realización del proyecto de investigación.

2. La determinación del nivel de necesidad para implementar</td></tr>
</table>

	3. Utilizar la metodología PPDIOO de cisco para un correcto trabajo de propuesta de implementación de un honeypot. 4. Realizar la simulación de un honeypot de seguridad informática en VirtualBox para controlar los ataques cibernéticos.	permitirá ver si es necesario o no la implementación del honeypot dentro de la agropecuaria Wilian & Roque S.R.L. 3. La utilización de la metodología PPDIOO de cisco permitirá trabajar de forma correcta nuestra investigación. 4. La realización de la simulación de un honeypot de seguridad informática en el VirtualBox permitirá tener una mejor opinión de lo que conviene trabajar con el honeypot.	

Fuente: Elaboración propia

4.9. Principios éticos

Durante el desarrollo de la presente investigación denominada "Propuesta de implementación de un honeypot de seguridad informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021" se ha tomado mucho en cuenta que se cumplan los principios éticos que nos brinda la ULADECH para que nuestra investigación sea original, por ello se cuenta con cinco principios (36).

Protección de la persona: Se debe tener el bienestar y la seguridad de las personas, respetando su dignidad, privacidad, confidencialidad, las creencias que la persona tiene; además se debe proteger los derechos fundamentales de cada uno (36).

Libre participación y derecho a estar informado: Todas las personas que están trabajando en el proyecto o desean trabajar en ellos debe ser por su voluntad propia; deben tener una opinión en lo que se hará y un anticipado aviso si se quiere hacer algunos cambios en el proyecto. Además, debe haber una equidad en el equipo y una integridad científica (36).

Beneficencia y no-maleficencia: En este principio no se debe causar daños y tener un riesgo-beneficio de manera positiva para que el bienestar y el cuidado sea seguro (36).

Cuidado del medio ambiente y respeto a la biodiversidad: Se debe tomar conciencia para evitar daños a los animales, plantas; al involucrar al medio ambiente ya que se puede evitar daños posteriores, por lo que se debe planificar acciones para minimizar los efectos y tener mayores beneficios (36).

Justicia: Lo que se busca con el investigador es tener justicia y un bien común para poder ejercer mis conocimientos con ideas razonables asegurando que no se establezca practicas injustas (36).

V. RESULTADOS

5.1. Resultados

a) Dimensión 1: Nivel de Importancia de una Seguridad Informática Honeypot

Tabla Nro. 3: Importancia de un software de seguridad informática

Distribución de frecuencia acerca de la importancia de un software de seguridad informática; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	20	100.00
No	-	-
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Considera importante que la Agropecuaria Wilian & Roque S.R.L. cuente con un software de seguridad informática?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 3 se puede observar que el 100.00% de la muestra seleccionada encuestada menciona que, SI considera importante que la agropecuaria Wilian & Roque S.R.L. cuente con un software de seguridad informática.

Tabla Nro. 4: Conocimiento de la herramienta honeypot

Distribución de frecuencia acerca del conocimiento de la herramienta honeypot; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	3	15.00
No	17	85.00
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Conoce usted sobre una herramienta honeypot para la seguridad informática en una empresa?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 4 se puede observar que el 85.00% de la muestra seleccionada encuestada menciona que, NO conoce sobre una herramienta honeypot para la seguridad informática en una empresa, mientras que un 15.00% que SI.

Tabla Nro. 5: Honeypot termina con peligros cibernéticos

Distribución de frecuencia acerca del honeypot que termina con peligros cibernéticos; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	17	85.00
No	3	15.00
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Piensa usted que un honeypot podría terminar con los peligros cibernéticos que vulneran los sistemas de la empresa?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 5 se puede observar que el 85.00% de la muestra seleccionada encuestada menciona que, SI piensa que un honeypot podría terminar con los peligros cibernéticos que vulneran los sistemas de la empresa, mientras que un 15.00% que NO.

Tabla Nro. 6: Importancia de conocer un honeypot

Distribución de frecuencia acerca de la importancia de conocer un honeypot; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	18	90.00
No	2	10.00
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Cree usted importante que las personas hoy en día deban conocer y utilizar un honeypot como seguridad en sus negocios?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 6 se puede observar que el 90.00% de la muestra seleccionada encuestada menciona que, SI creen importante que las personas hoy en día deban conocer y utilizar un honeypot como seguridad en sus negocios, mientras que un 10.00% que NO.

Tabla Nro. 7: Honeypot ayuda a mantener seguros los datos

Distribución de frecuencia acerca de honeypot que ayuda a mantener seguros los datos; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	16	80.00
No	4	20.00
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Considera que el análisis de un honeypot ayude a mantener la seguridad de sus datos en la empresa?

Aplicado por: Terrones V.; 2020

En la Tabla Nro. 7 se puede observar que el 80.00% de la muestra seleccionada encuestada menciona que, SI considera que el análisis de un honeypot ayude a mantener la seguridad de sus datos en la empresa, mientras que un 20.00% que NO.

Tabla Nro. 8: Robos y amenazas en los sistemas

Distribución de frecuencia acerca de robos y amenazas en los sistemas; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	7	35.00
No	13	65.00
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Conoce o a escuchado sobre alguna empresa que ha sufrido de robos o amenazas en sus sistemas?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 8 se puede observar que el 65.00% de la muestra seleccionada encuestada menciona que, NO conoce o a escuchado sobre alguna empresa que ha sufrido de robos o amenazas en sus sistemas, mientras que un 35.00% que SI.

Tabla Nro. 9: Ventajas de un honeypot

Distribución de frecuencia acerca de ventajas de un honeypot; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	18	90.00
No	2	10.00
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Cree que un honeypot traería mucha ventaja para la Agropecuaria Wilian & Roque S.R.L.?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 9 se puede observar que el 90.00% de la muestra seleccionada encuestada menciona que, SI creen que un honeypot traería mucha ventaja para la Agropecuaria Wilian & Roque S.R.L., mientras que un 10.00% que NO.

Tabla Nro. 10: Formas de ser atacado un sistema

Distribución de frecuencia acerca de las formas de ser atacado un sistema; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	3	15.00
No	17	85.00
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Usted conoce de qué forma puede ser atacado un sistema?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 10 se puede observar que el 85.00% de la muestra seleccionada encuestada menciona que, NO conoce de qué forma puede ser atacado un sistema, mientras que un 15.00% que SI.

Tabla Nro. 11: Consecuencias de ataques cibernéticos

Distribución de frecuencia acerca de consecuencias de ataques cibernéticos; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	8	40.00
No	12	60.00
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Conoce usted que resultados o consecuencias puede traer los ataques cibernéticos?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 11 se puede observar que el 60.00% de la muestra seleccionada encuestada menciona que, NO conoce que resultados o consecuencias puede traer los ataques cibernéticos, mientras que un 40.00% que SI.

Tabla Nro. 12: Amenazas de ataques cibernéticos

Distribución de frecuencia acerca de amenazas de ataques cibernéticos; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	19	95.00
No	1	5.00
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Consideras que los ataques cibernéticos son una amenaza para el desarrollo de una empresa?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 12 se puede observar que el 95.00% de la muestra seleccionada encuestada menciona que, SI consideran que los ataques cibernéticos son una amenaza para el desarrollo de una empresa, mientras que un 5.00% de los encuestados mencionan que NO.

Tabla Nro. 13: Resumen de la Dimensión Nro. 1

Resumen de la Dimensión de la importancia de una seguridad informática; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	13	65.00
No	7	35.00
Total	20	100.00

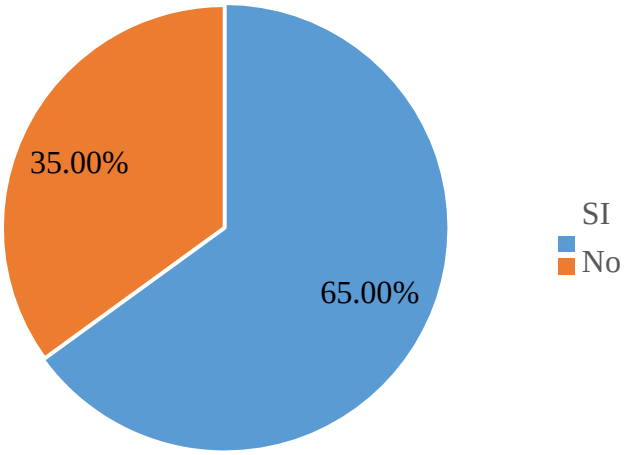
Fuente: Cuestionario aplicado a los trabajadores y clientes respecto a la dimensión Nro. 1.

Aplicado por: Terrones V; 2020

En la Tabla Nro. 13 se puede observar que el 65.00% de los trabajadores y clientes SI consideran importante una seguridad informática, mientras que un 35.00% afirma que NO.

Gráfico Nro. 7: Resumen de la dimensión Nro. 1

Resumen de la Dimensión de la importancia de una seguridad informática honeypot; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.



Fuente: Tabla Nro. 11

b) Dimensión 2: Necesidad para implementar un honeypot

Tabla Nro. 14: Beneficios de implementar un honeypot

Distribución de frecuencia acerca de los beneficios para implementar un honeypot; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	18	90.00
No	2	10.00
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Cree usted que sería beneficioso implementar un honeypot en la empresa?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 14 se puede observar que el 90.00% de la muestra seleccionada encuestada menciona que, SI creen que sería beneficioso implementar un honeypot en la empresa, mientras que un 10.00% que NO.

Tabla Nro. 15: Estabilidad y seguridad con honeypot

Distribución de frecuencia acerca de la estabilidad y seguridad con honeypot; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	20	100.00
No	-	-
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Considera importante que los datos de la empresa mantengan una estabilidad y seguridad?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 15 se puede observar que el 100.00% de la muestra seleccionada encuestada menciona que, SI consideran importante que los datos de la empresa mantengan una estabilidad y seguridad.

Tabla Nro. 16: El software reduce vulnerabilidades

Distribución de frecuencia el software reduce vulnerabilidades; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	19	95.00
No	1	5.00
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Cree que el desarrollo de la implementación de un software de seguridad informática reduciría las vulnerabilidades que mantiene algunas empresas?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 16 se puede observar que el 95.00% de la muestra seleccionada encuestada menciona que, SI creen que el desarrollo de la implementación de un software de seguridad informática reduciría las vulnerabilidades que mantiene algunas empresas, mientras que un 5.00% de los encuestados mencionan que NO.

Tabla Nro. 17: Importancia para implementar seguridad

Distribución de frecuencia acerca de la importancia para implementar seguridad; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	20	100.00
No	-	-
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Sera importante que hoy en día las empresas implementen una seguridad para sus sistemas como un honeypot?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 17 se puede observar que el 100.00% de la muestra seleccionada encuestada menciona que, SI será importante que hoy en día las empresas implementen una seguridad para sus sistemas como un honeypot.

Tabla Nro. 18: Conocimiento de perdida de información

Distribución de frecuencia acerca del conocimiento de perdida de información; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	3	15.00
No	17	85.00
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Conoce usted de algún problema que ha mantenido la empresa sobre una pérdida de información?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 18 se puede observar que el 85.00% de la muestra seleccionada encuestada menciona que, NO conoce de algún problema que ha mantenido la empresa sobre una pérdida de información, mientras que un 15.00% que SI.

Tabla Nro. 19: La implementación reduce pérdidas económicas

Distribución de frecuencia acerca de la implementación reduce pérdidas económicas; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	15	75.00
No	5	25.00
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Considera importante que hoy en día con la implementación de un honeypot no habría pérdidas económicas?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 19 se puede observar que el 75.00% de la muestra seleccionada encuestada menciona que, SI consideran importante que hoy en día con la implementación de un honeypot no habría pérdidas económicas, mientras que un 25.00% que NO.

Tabla Nro. 20: Avances tecnológicos hace crecer ataques cibernéticos

Distribución de frecuencia acerca de los avances tecnológicos hacen crecer ataques cibernéticos; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si No	20	100.00
Total	-	-
	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Cree usted que el avance de la tecnología está haciendo que los ataques cibernéticos crezcan?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 20 se puede observar que el 100.00% de la muestra seleccionada encuestada menciona que, SI creen que el avance de la tecnología está haciendo que los ataques cibernéticos crezcan.

Tabla Nro. 21: Mantener seguro la información

Distribución de frecuencia acerca de mantener seguro la información; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si No	20	100.00
Total	-	-
	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Considera que la agrícola debería dedicarse no solo en ventas sino en mantener seguro su información?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 21 se puede observar que el 100.00% de la muestra seleccionada encuestada menciona que, SI consideran que la agrícola debería dedicarse no solo en ventas sino en mantener seguro su información.

Tabla Nro. 22: Honeypot beneficia a empresa y clientes

Distribución de frecuencia acerca de honeypot beneficia a empresa y clientes; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	18	90.00
No	2	10.00
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Considera que la implementación de un honeypot sea beneficioso para la empresa y sus clientes?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 22 se puede observar que el 90.00% de la muestra seleccionada encuestada menciona que, SI consideran que la implementación de un honeypot sea beneficioso para la empresa y sus clientes, mientras que un 10.00% que NO.

Tabla Nro. 23: Seguridad estable en sus sistemas

Distribución de frecuencia acerca de la seguridad estable en sus sistemas; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	9	45.00
No	11	55.00
Total	20	100.00

Fuente: Instrumento aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L.; respecto a la pregunta ¿Cree usted que la empresa mantenga una seguridad estable y conforme con sus sistemas hoy en día?

Aplicado por: Terrones V; 2020

En la Tabla Nro. 23 se puede observar que el 55.00% de la muestra seleccionada encuestada menciona que, NO creen que la empresa mantenga una seguridad estable y conforme con sus sistemas hoy en día, mientras que un 45.00% que SI.

Tabla Nro. 24: Resumen de la Dimensión Nro. 2

Resumen de la Dimensión de la necesidad para implementar un honeypot; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Alternativas	n	%
Si	16	80.00
No	4	20.00
Total	20	100.00

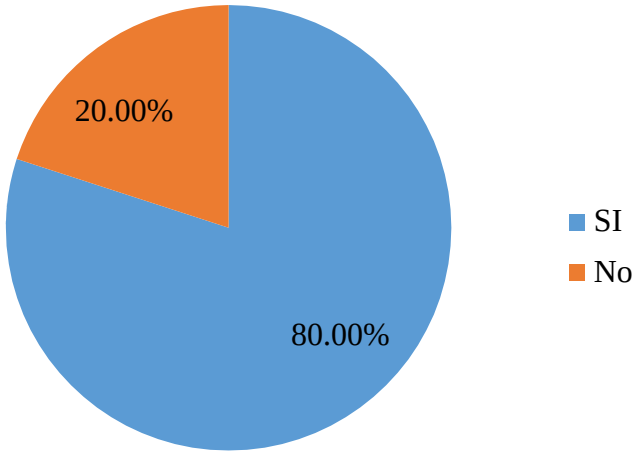
Fuente: Cuestionario aplicado a los trabajadores y clientes respecto a la dimensión Nro. 2.

Aplicado por: Terrones V; 2020

En la Tabla Nro. 24 se puede observar que el 80.00% de los trabajadores y clientes SI consideran la necesidad para implementar un honeypot, mientras que un 20.00% afirma que NO.

Gráfico Nro. 8: Resumen de la dimensión Nro. 2

Resumen de la Dimensión de la necesidad para implementar un honeypot; respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.



Fuente: Tabla Nro. 24

Tabla Nro. 25: Resumen general de dimensiones

Resumen general de dimensión, respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

DIMENSIONES	Si		No		Total	
	n	%	n	%	n	%
Nivel de importancia de una seguridad informática honeypot	13	65.00	7	35.00	20	100.00
Nivel de necesidad para implementar un honeypot	16	80.00	4	20.00	20	100.00

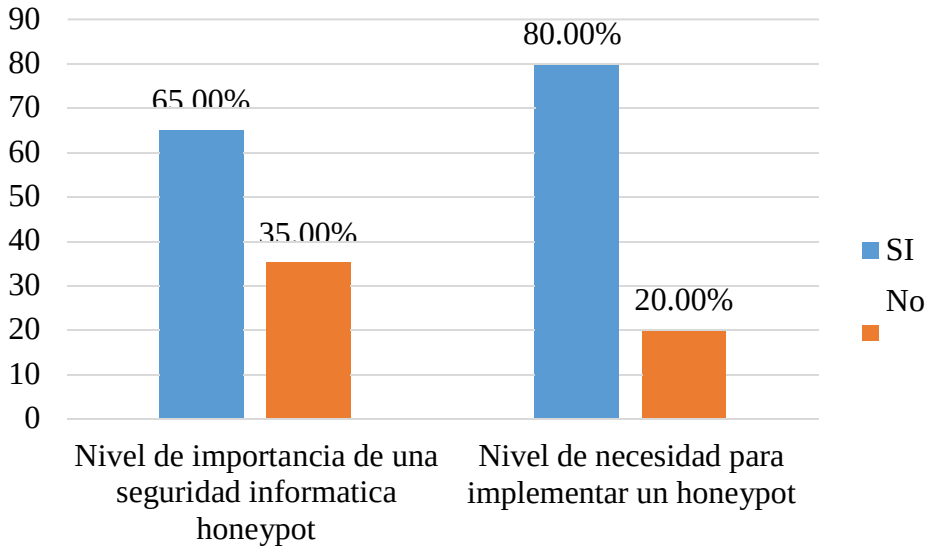
Fuente: Cuestionario aplicado a los trabajadores y clientes de la Agropecuaria Wilian & Roque S.R.L., respecto al resumen general de las 2 dimensiones.

Aplicado por: Terrones V; 2020

En la Tabla Nro. 25, se observa que en la primera dimensión el mayor porcentaje de los encuestados es SI, en relación a la dimensión de nivel de importancia de una seguridad informática honeypot, en la segunda dimensión el mayor porcentaje es SI, en relación a la dimensión de nivel de necesidad para implementar un honeypot.

Gráfico Nro. 9: Resumen general de dimensiones

Resumen general de dimensión, respecto a la Propuesta de Implementación de un Honeypot de Seguridad Informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.



Fuente: Tabla Nro. 25

5.2. Análisis de resultados

El objetivo general de esta investigación es realizar la propuesta de implementación de un honeypot de seguridad informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021, con la finalidad de controlar los ataques cibernéticos. En el cual se ha realizado en dos dimensiones que son importancia de una seguridad informática honeypot y necesidad para implementar un honeypot. Por consiguiente, después de haber interpretado los resultados se proceden a analizar los siguientes párrafos:

1. En lo que respecta a la dimensión: Importancia de una Seguridad Informática Honeypot, la Tabla Nro. 11, se puede observar que el 65.00% de trabajadores y clientes encuestados expresaron que, SI creen importante que debe haber una seguridad informática como un honeypot en la Agropecuaria Wilian & Roque S.R.L. ,mientras que el 35.00% de los encuestados indicó que NO creen importante que debe haber una seguridad informática como un honeypot, este resultado es similar a los autores Flores y Quintana (3), en su tesis titulada "Sistema de detección de ataques informáticos a redes de datos empresariales soportado en honeypots" en el año 2018, que indico el 66.00% cree que es muy importante el honeypot ya que ayuda al análisis de información sobre los ataques cibernéticos identificando los requisitos, la arquitectura y realizando las pruebas necesarias para probar la funcionalidad del honeypot.

2. En lo que respecta a la dimensión: Necesidad para implementar un honeypot, la Tabla Nro. 22, se puede observar que el 80.00% de trabajadores y clientes encuestados expresaron que, SI sienten la necesidad de implementar un honeypot en la Agropecuaria Wilian & Roque S.R.L. , mientras que el 20.00% de los encuestados indicaron que NO es necesario implementar un honeypot, este resultado es similar a el autor Matus (5), en su trabajo de tesis titula "Análisis e

implementación de una solución honeypot para un entorno experimental" en el año 2017; muestra como resultados que el 90.00% estuvo de acuerdo que haga la implementación del honeypot ya que es muy necesario, y el 10.00% no. sus objetivos de esta investigación fue configurar e implementarlo las diferentes soluciones de un honeypot en Linux con riesgos experimentales, hacer las instalaciones y configuraciones para emplear en una cámara de pruebas, realizando ataques para ver si funciona correctamente las funciones del honeypot.

5.3. Propuesta de mejora

Después de hacer todo el estudio correspondiente de mi investigación que se obtuvo con resultados ya mostrados, con la aplicación de la técnica e instrumento de recolección de datos y del análisis que hice a cada trabajador y cierta cantidad de clientes de la empresa Agropecuaria Wilian & Roque S.R.L. encuestándolos, me vi con la necesidad de hacer una propuesta de mejora que ayudará a combatir a los ataques cibernéticos con el apoyo del honeypot. Este estudio puede ayudar a crear un nuevo proyecto de investigación a un futuro por el motivo de que nadie está libre de ser vulnerado por una mala persona que desea robar información.

Con el apoyo de la metodología PPDIOO de cisco se desarrolla mi propuesta de mejora para esta investigación, ya que esta ayuda a definir las 6 fases que se requiere para poder realizar mi estudio usando el honeypot, dentro de mi proyecto de investigación. Entre estas fases son las siguientes:

Tabla Nro. 26: Metodología PPDIOO

METODOLOGÍA PPDIOO	
FASES	**FUNCIONES**
Preparar	En esta fase se hará un pequeño estudio del problema que existe dentro de la empresa.
Planear	En esta fase se identifican los requerimientos que se usan para hacer el honeypot.
Diseñar	En esta fase se visualiza la topología de red y los diagramas de los procesos que se necesitan.
Implementar	En esta fase se observa las interfaces que se logró realizar al momento de realizar el honeypot.
Operar	En esta fase se incluye el mantenimiento y el monitoreo del honeypot.
Optimizar	En esta fase se puede realizar modificaciones si se les necesita o resolviendo a la brevedad si existe algún inconveniente con el honeypot.

Fuente: Elaboración propia.

Para ello solo usaremos hasta la fase de implementar ya que mi investigación solo necesita hasta esa fase. Por ende, se dará solución a nuestro problema planteado ¿De qué manera la propuesta de implementación de un honeypot de seguridad informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2020, mejora el control de los ataques cibernéticos?

5.3.1. Preparar

En esta primera fase nos ayuda a que se llegue a analizar la problemática que se observa en la actualidad dentro de la Agropecuaria Wilian & Roque S.R.L. y además se conoce que también está afectando a nivel nacional e internacional en todas las empresas ya que en todo momento hay personas con malas intenciones que viene robando información por ello, se viene escuchando sobre robo de información cibernética y esto es muy peligroso ya que esta situación afecta bastante a cualquier persona o empresa. Por ello se planteó usar esta herramienta honeypot ya que va a consistir en controlar los ataques cibernéticos que están causando daño que viene perjudicando a mucha gente. Esto se empezó haciendo las respectivas encuestas y haciendo averiguaciones de la empresa y temas relacionadas a la seguridad informática para poder analizar los riesgos que existen.

Actualmente la Agropecuaria Wilian & Roque S.R.L. no cuenta con un sistema de seguridad dentro de sus instalaciones de su tienda que ayuden a mantener seguro las ventas e información que esta tiene de sus productos y ganancias del día, además de sus datos muy importantes. Por ello se realizó este proyecto de investigación que dará solución al problema de la seguridad informática ya que hoy en día la ciberdelincuencia está muy de moda y está causando graves problemas de pérdidas económicas y datos de información.

5.3.2. Planear

Requerimiento Funcional

Tabla Nro. 27: Lista de requerimiento funcional

CODIGO	DESCRIPCIÓN
RF1	Permiso del acceso al honeypot.
RF2	Configuraciones para instalar un honeypot
RF3	Instalación.
RF4	Escanear todas las funcionalidades
RF5	Visualizar las estadísticas de ataques.
RF6	Realizar los analices de las alertas.
RF7	Reporte de los ataques.
RF8	Procesar toda la información de los ataques.

Fuente: Elaboración Propia

Requerimiento No Funcional

Tabla Nro. 2826: Lista de requerimiento no funcional

ID	DESCRIPCIÓN
RNF1	Los permisos que se dan solo pueden ser modificado por el administrador.
RNF2	Facilidad en el uso.
RNF3	Confiabilidad del honeypot
RNF4	Honeypot mantiene la eficiente seguridad.
RNF5	Honeypot es adaptable a distintos sistemas operativos.

Fuente: Elaboración Propia

Requerimientos de Software

Para este informe de investigación se utiliza los siguientes programas:

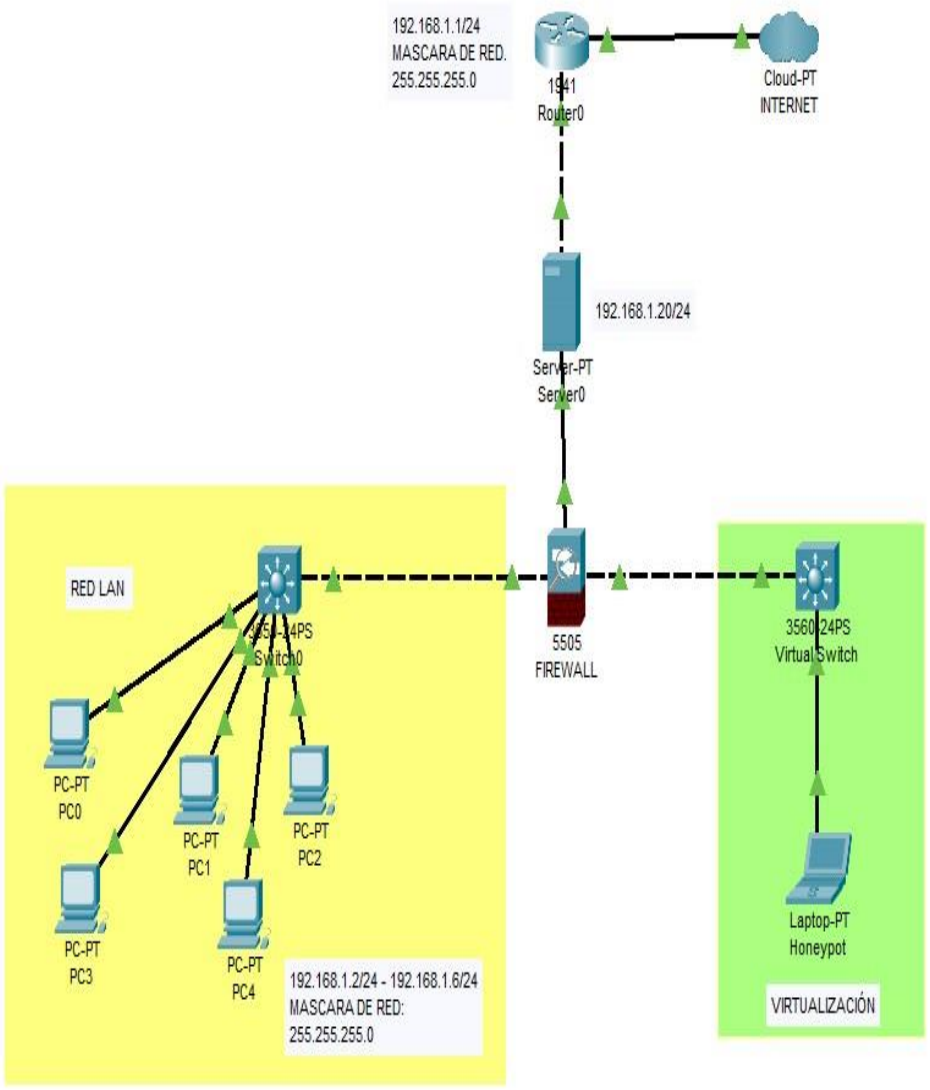
ID	DESCRIPCIÓN
RS1	VirtualBox
RS2	Honeydrive

Fuente: Elaboración propia

5.3.3. Diseñar

5.3.3.1. Topología de red con honeypot

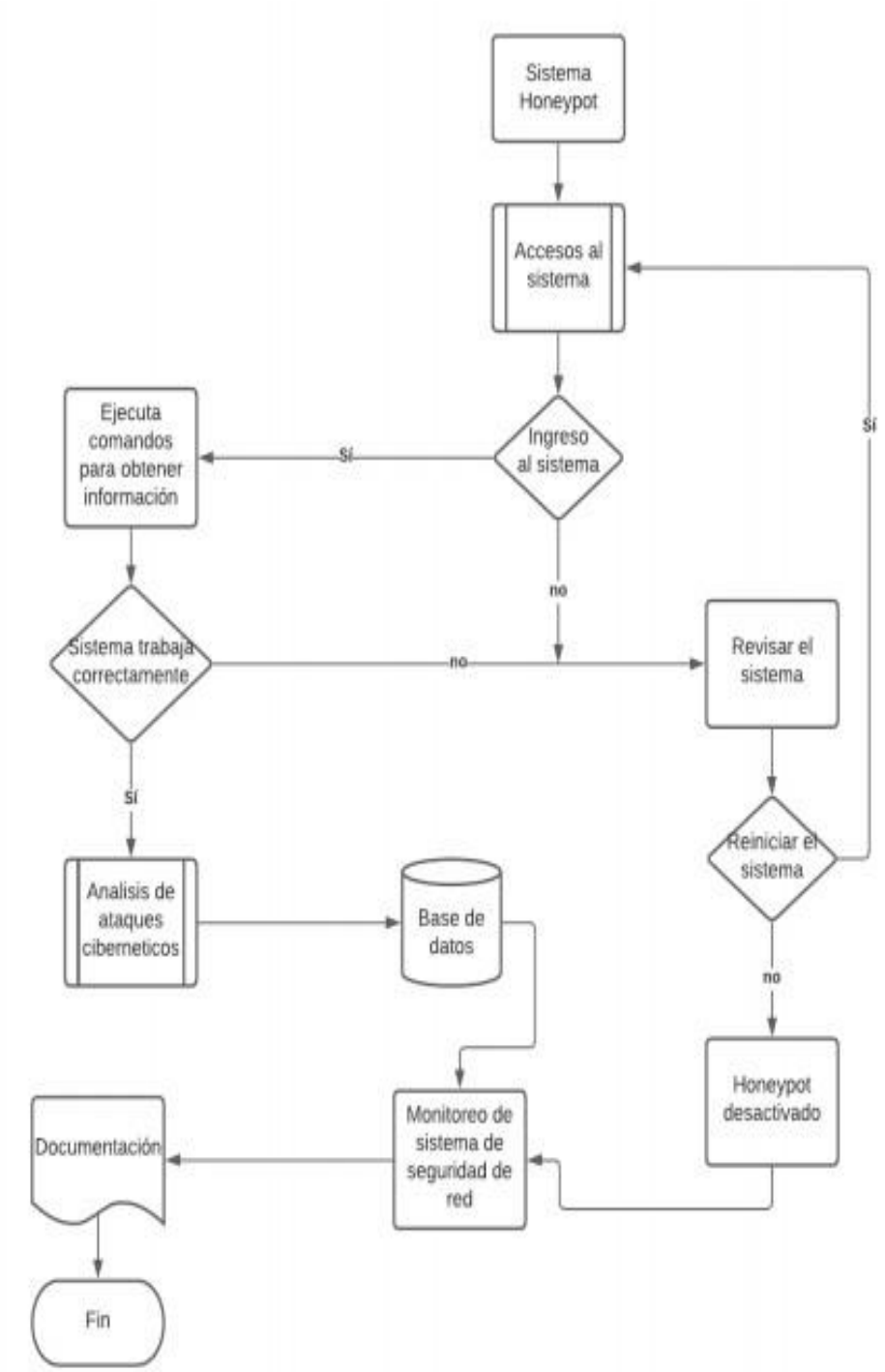
Gráfico Nro. 10: Topología de red con honeypot



Fuente: Elaboración propia

5.3.3.2. Diseño de un diagrama de flujo

Gráfico Nro.11: El diagrama de flujo del sistema honeypot



Fuente: Elaboración Propia.

En el gráfico Nro. 07 pude observar el diagrama de flujo anterior, ya que se establece varias actividades que ayudan a tener una mejor visión de lo que trato de hacer y la finalidad de ayudar gracias al monitorear la red con el honeypot. El diagrama de flujo ayuda al administrador a tener claro lo que él tiene a cargo como iniciar el honeypot y donde termina este, es por ello que pensé realizar y mejorar y poder dar una buena solución de lo que se hace y también desarrollar la documentación en un informe que finalmente se presenta al gerente general de la agropecuaria Wilian & Roque.

5.3.3.3. Desarrollo de los diagramas de procesos

Definición de participantes

Para mi sistema propuesto se identificó los siguientes participantes:

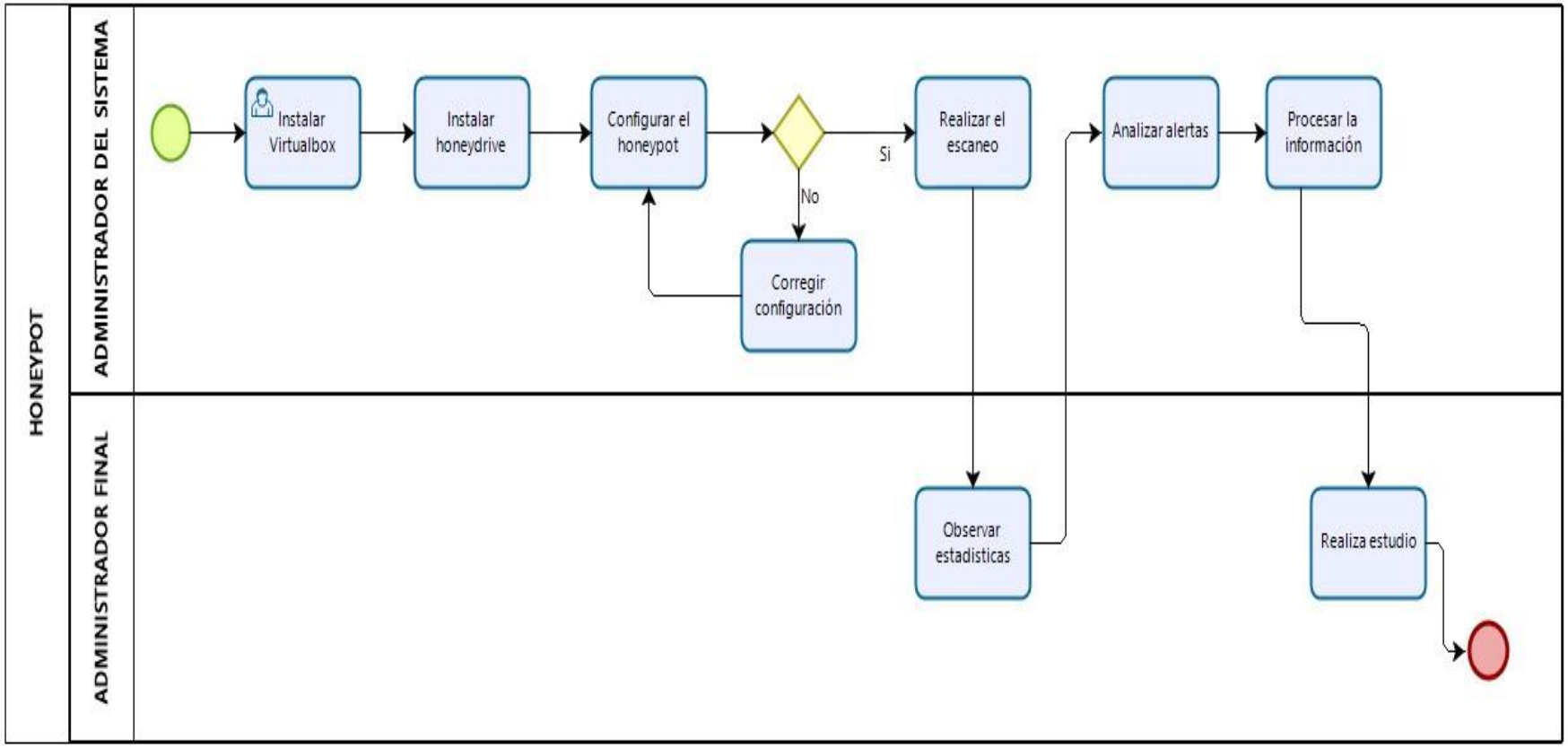
- **Administrador de sistemas:**

  Este se encarga de hacer la instalación y además de instalar y realizar aquellas configuraciones que se necesitan para crear nuestro honeypot, también este participante debe saber y conocer de las funcionalidades del sistema al revés y al derecho.

- **Administrador final:**

  Este se encarga de hacer reportes de ataques gracias a las revisiones de estadística que se hace al honeypot, por ello este participante es como el usuario final ya que visualizara todos los ataques que se vendrá dando dentro del honeypot que ayudara a mejorar nuestra seguridad informática.

Gráfico Nro. 12: Diagrama del procedimiento para un honeypot



Fuente: Elaboración propia

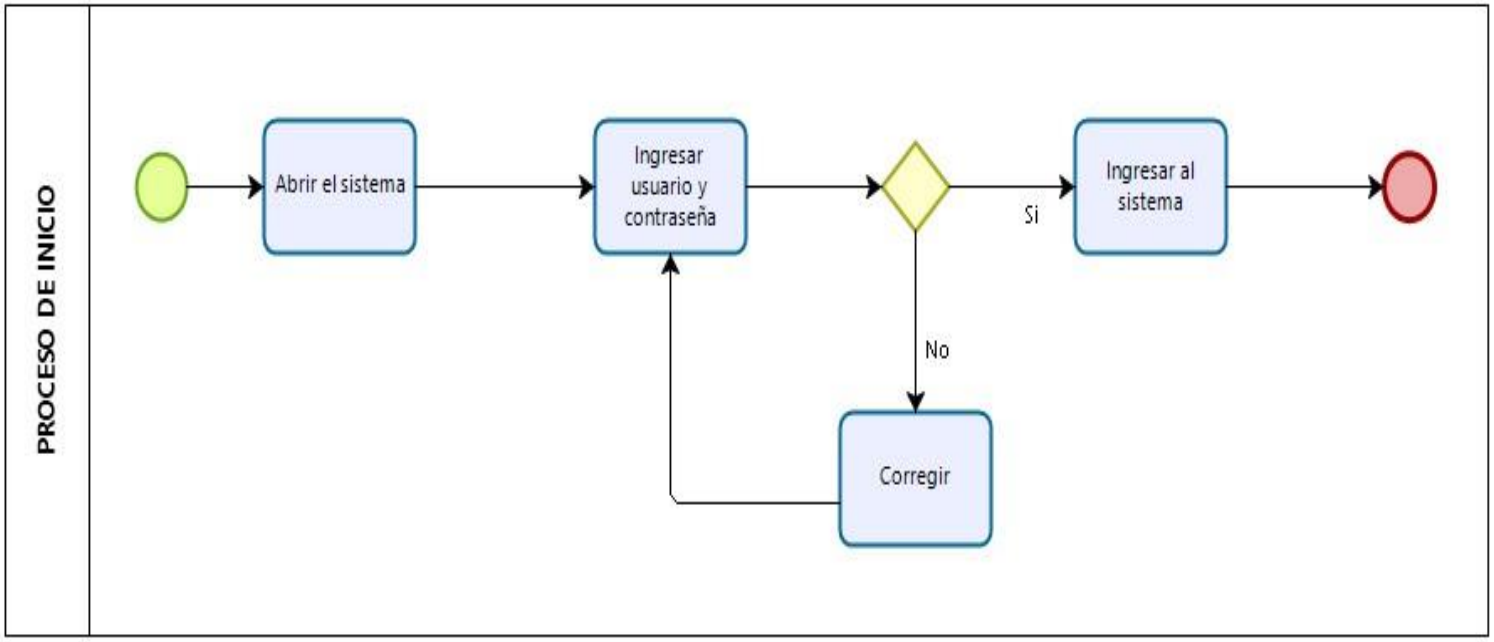
Tabla Nro. 279: Diagrama del procedimiento para un honeypot

TAREA	**DEFINICIÓN**
Instalar VirtualBox	Lo primero que se debe hacer es instalar correctamente el VirtualBox, una máquina virtual que ayudará a simular dentro de la computadora en que se realizará la investigación.
Instalar honeydrive	Se deberá tener este archivo descargado y debemos instalar dentro del VirtualBox.
Configurar el honeypot	Luego se debe realizar las configuraciones con comandos dentro del terminal del VirtualBox para lograr realizar el honeypot.
Corregir configuración	Si por un caso nos equivocamos al hacer alguna configuración se puede corregir rápidamente dentro del terminal con códigos para seguir con la siguiente tarea.
Realizar el escaneo	Ya listo la instalación del honeypot, se debe realizar correctamente el escaneo de los ataques si está ocurriendo en ese momento.
Observar estadísticas	En la pantalla después de realizar el escaneo se visualizará las estadísticas que se logró

	descubrir que ayudan a tener una mejor visualización del escaneo.
Analizar alertas	Si se observa riesgos en las estadísticas se debe analizar minuciosamente cada uno de ellas de los ataques cibernéticos.
Procesar información	Después de haber analizado las alertas se debe procesar toda esta información que se logró reunir al hacer el escaneo.
Realizar estudio	Al finalizar todo esto se puede obtener información valiosa y por ello se puede hacer un estudio profundo con la finalidad de lograr controlar los ataques cibernéticos que dañen a la agropecuaria Wilian & Roque.

Fuente: Elaboración propia

Gráfico Nro. 13: Diagrama del procedimiento del inicio



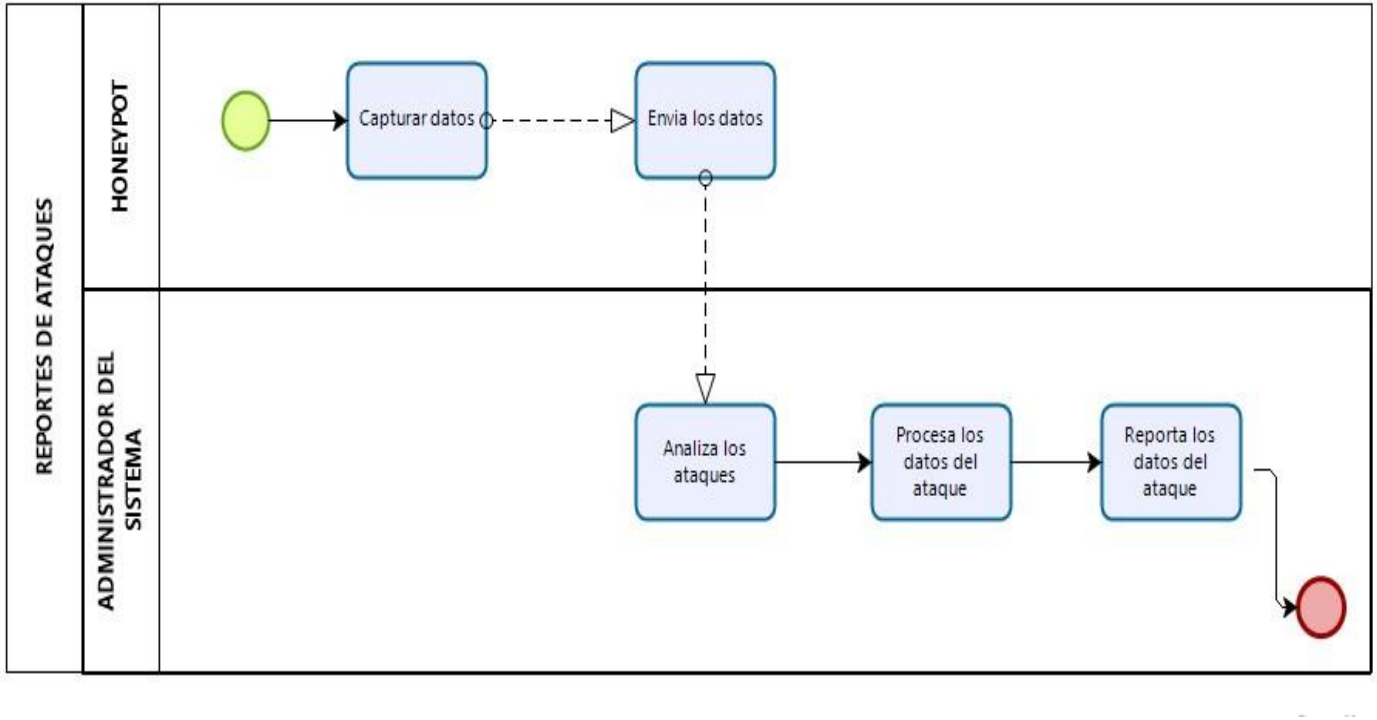
Fuente: Elaboración propia

Tabla Nro. 30: Diagrama del procedimiento del inicio

TAREA	**DEFINICIÓN**
Abrir el sistema	Lo primero que se debe hacer al querer ingresar al honeypot es abrir el sistema dentro del VirtualBox.
Ingresar usuario y contraseña	El administrador debe ingresar su usuario y contraseña que se le asigno para poder entrar dentro del honeypot para poder trabajar dentro de este.
Corregir	Si por algún motivo el administrador ingresa mal su usuario y contraseña deberá corregir e ingresar de nuevo su usuario y contraseña nuevamente.
Ingresar al sistema	Si se logra escribir correctamente el usuario y contraseña ya el administrador podrá ingresar al honeypot y realizar todas las actividades que este pueda realizar, como escanear o las visualizaciones de estadísticas de todos los ataques cibernéticos.

Fuente: Elaboración propia

Gráfico Nro. 14: Diagrama del proceso de los reportes de ataques



Fuente: Elaboración propia

Tabla Nro. 31: Diagrama del proceso de los reportes de ataques

TAREA	**DEFINICIÓN**
Capturar datos	En este momento al escanear los ataques cibernéticos dentro del honeypot se podrá capturar todos los datos del ciberdelincuente que quiere ingresar a robar información de la agropecuaria Wilian & Roque.
Envía los datos	Después del escaneo se debe capturar la información y enviar todos los datos que se obtuvieron a un lugar que guarde completamente toda esta información.
Analiza los ataques	Se debe analizar completamente los ataques ya que el administrador puede hacer todas estas actividades y visualizar la ubicación ip de la persona que quiere robar la información de la empresa.
Procesa los datos del ataque	Se debe procesar toda la información y los datos que se vino adquiriendo de todos los ataques cibernéticos.
Reporta los datos del ataque	Se reportarán los datos de todos los ataques que se viene dando dentro de la empresa.

Fuente: Elaboración propia

5.3.4. Implementar

En esta fase se trabaja todo lo que es las configuraciones que se tiene que hacer para lograr una completa instalación del honeypot dentro de VirtualBox. Se observará todas las interfaces del honeypot que nos permitirá tener un mejor control de los ataques cibernéticos que quieren vulnerar a la empresa, buscando infamación valiosa que le pueda servir de algo para robar a la Agropecuaria Wilian & Roque S.R.L.

- Realizamos la instalación del honeypot (Kippo SSH)

Primero se debe descargar el honeyDrive en cualquier navegador web y tenerlo guardado en una ruta específica, para ser encontrada con facilidad.

Luego haremos el uso de la máquina virtual VirtualBox para ejecutar nuestro archivo honeydrive. Y le damos en Iniciar para ejecutar nuestro honeypot.

Gráfico Nro. 15: Interfaz de la instalación del honeyDrive.

Para poder activar todos los servicios que son necesarias para el buen funcionamiento de este honeypot, se debe ingresar los siguientes comandos en el terminal del honeyDrive.

```
honeydrive@honeydrive:/honeydrive/kippo$ gedit kippo.cfg
```

Le damos enter y nos aparecerá unas configuraciones para ingresar la dirección de nuestro nuevo servidor y el puerto dentro del Kippo.

```
ssh_addr = 192.168.8.9
ssh_port = 22
```

Después de estos pasos ya tendremos nuestro puerto, la dirección, todo esto dentro del servidor falso en Kippo.

```
honeydrive@honeydrive:/honeydrive/kippo$ gedit kippo.cfg.dist
```

```
ssh_addr = 192.168.8.9
ssh_port = 22
hostname = SVRHONEYATACADO
```

Finalmente, al realizar todas las configuraciones en el perfil que ingresamos dentro de la DMZ la cual siempre se encuentra protegida por Firewall. Todas las configuraciones se encontrarán ubicadas con el nombre readme.txt dentro del honeyDrive.

Para poder inicializar el honeypot se transcribe el siguiente comando:

```
honeydrive@honeydrive:/honeydrive/kippo$ ./start.sh
```

Para realizar las comprobaciones necesarias si están en buen funcionamiento el honeypot y ya está realizando las medidas de seguridad y controlar los ataques cibernéticos. Se debe ingresar el siguiente comando dentro del navegador del honeyDrive:

192.168.8.9/kippo-graph

Esto nos mostrará directamente la interfaz de honeypot (Kippo-graph) que estará en funcionamiento y nos mostrará con que honeypot estamos trabajando.

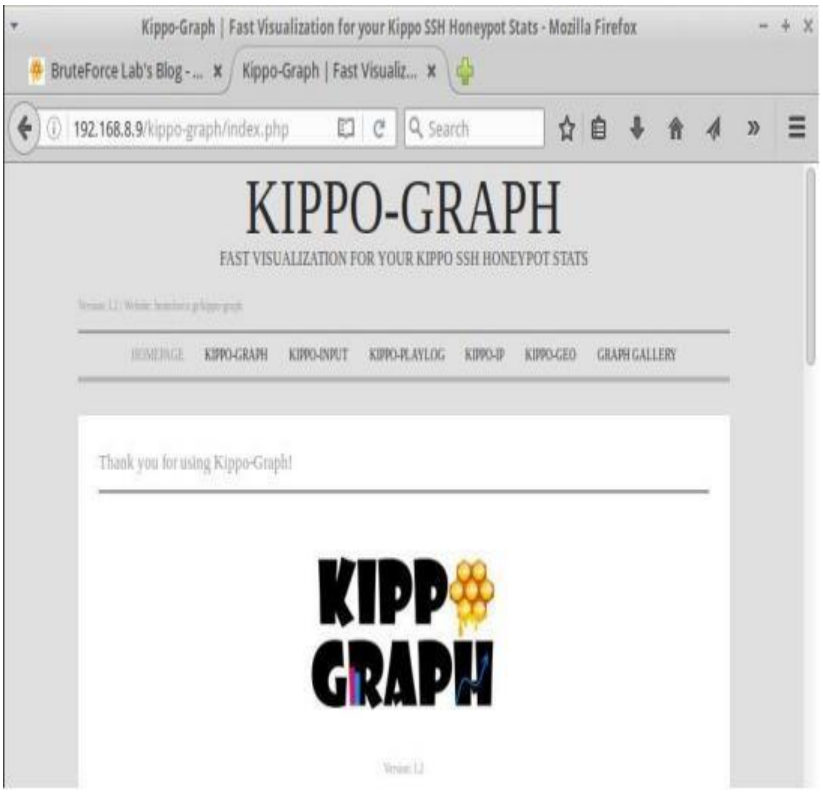


Gráfico Nro. 16: Interfaz gráfica del honeypot Kippo-Graph.

En estas siguientes interfaces se mostrará las diferentes pestañas que nos brinda Kippo graph para poder rastrear a los atacantes que quieren robarnos información o quieran ingresar dentro de nuestra red.

En el siguiente gráfico nos muestra un diagrama de barras y un diagrama circular que muestra los porcentajes en que se están realizando los ataques cibernéticos.

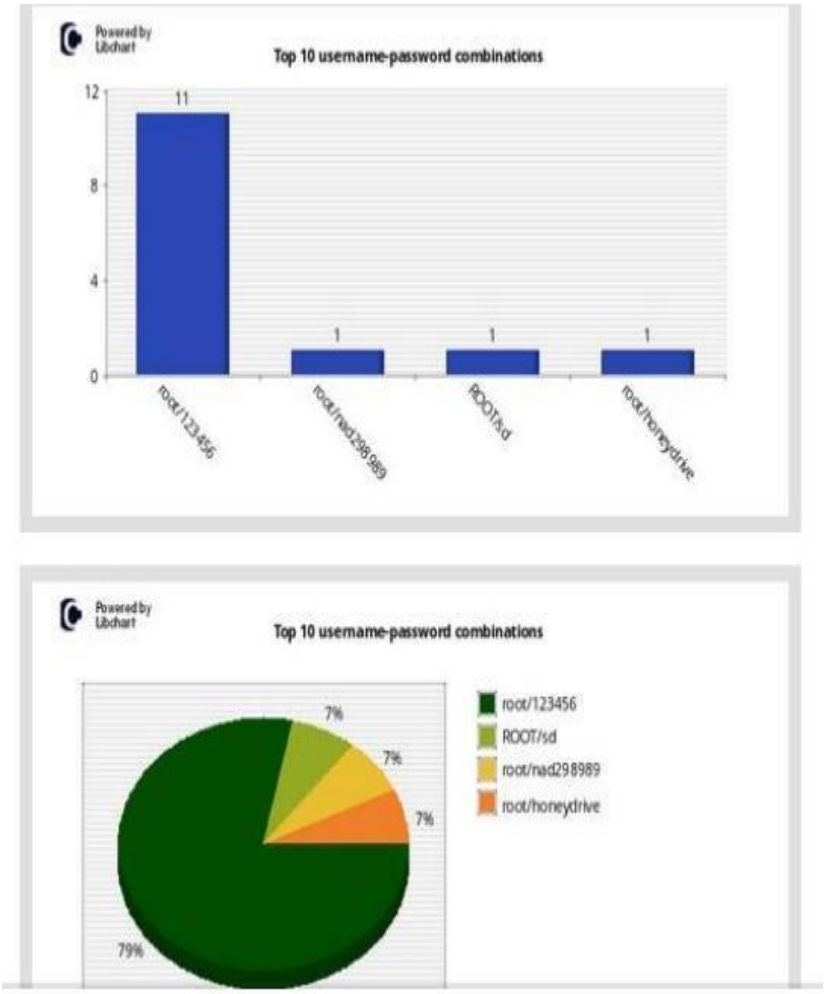


Gráfico Nro. 17: Interfaz gráfica a través de porcentajes de los ataques cibernéticos.

A continuación, se muestran dentro de este grafico las conexiones en SSH que hicieron los atacantes y visualizar dentro de esta interfaz.

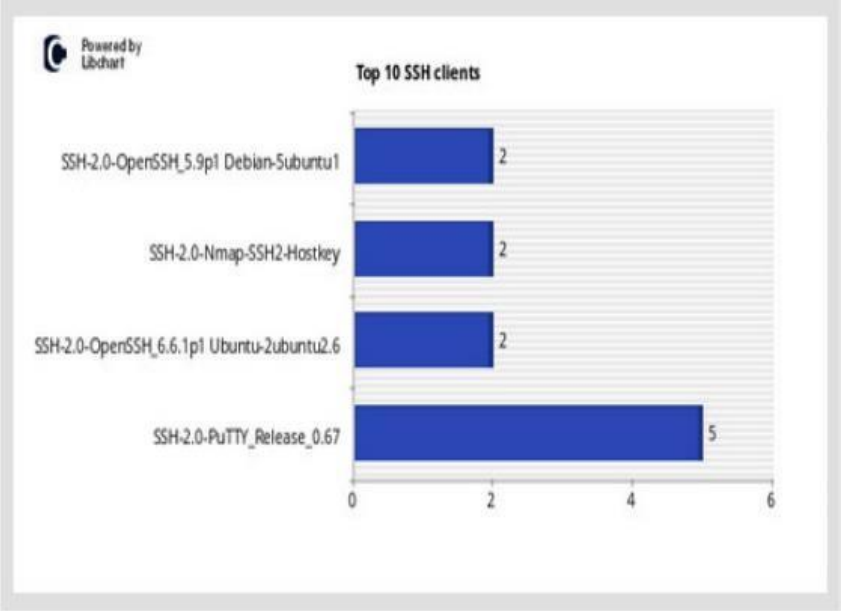


Gráfico Nro. 18: Conexiones de SSH de los atacantes.

En esta otra grafica se podrá rastrear al atacante gracias a que se guarda la dirección IP desde donde se ubica y además la ciudad entre otros datos.

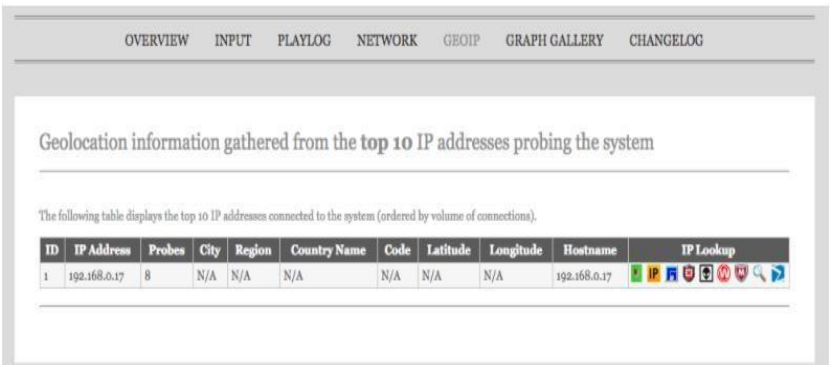


Gráfico Nro. 19: La dirección ip del que nos quiere atacar.

5.3.5. Operar

Se debería mantener el honeypot en constante monitoreo para verificar que no ocurra ningún problema ya que esto perjudicaría bastante a la empresa. Esto se tendría que hacer cada cierto tiempo, que será planteado al dueño de esta empresa y si acepta pues será beneficioso para la clientela y empresa.

5.3.6. Optimizar

Se sugeriría que el honeypot tenga la opción de una mejora continua dentro de la empresa, sin que se vea afectado su función de monitoreo del honeypot en la Agropecuaria Wilian & Roque S.R.L.

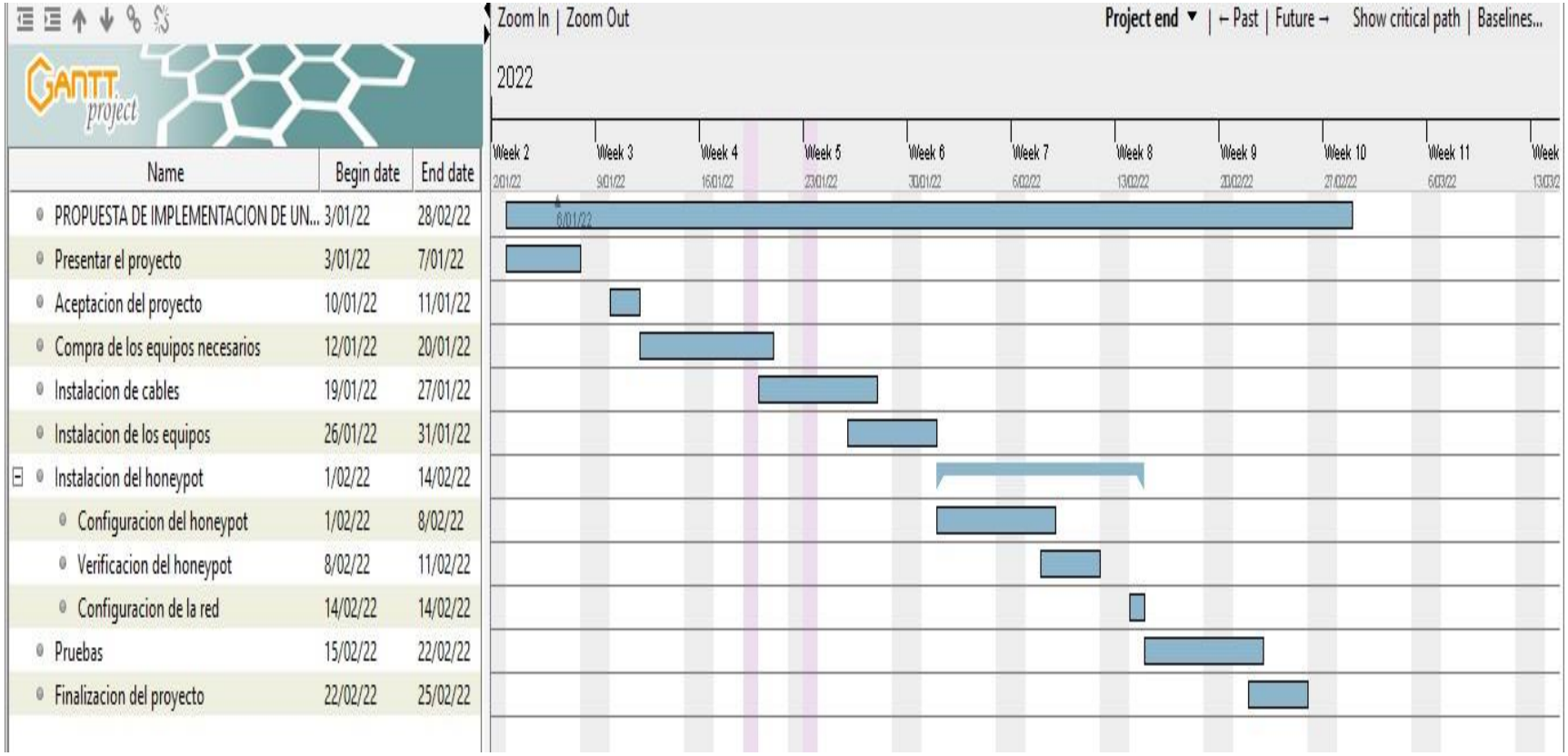
5.3.7. Presupuesto

Tabla Nro. 32: Presupuesto

Cantidad	Nombre	Características	Costo (S/)
1	Mano de obra	Ingeniero de sistemas	1500.00
1	Virtual Box	Ultima versión	-
1	HoneyDrive	Ultima versión	-
PRECIO TOTAL			1500.00

Fuente: Elaboración propia

5.3.8. Cronograma de actividades para la propuesta de implementación



Fuente: Elaboración propia

VI. CONCLUSIONES

Según los resultados obtenidos con este estudio, luego de ser interpretados y analizados se puede observar que se requiere la necesidad de contar con un software de seguridad informática como es el honeypot para cuidar a la Agropecuaria Wilian & Roque S.R.L. para reducir los riesgos de ser atacado por un ciberdelincuente; de esta manera se vio la necesidad de realizar la propuesta de implementación de un honeypot de seguridad informática en la agropecuaria Wilian & Roque – Chimbote; 2021, con la finalidad de controlar los ataques cibernéticos.

Respecto a todo el estudio se puede concluir lo siguiente:

1. Se determinó que el nivel de importancia con respecto a una seguridad informática honeypot si es gran interés, como nos muestra el resultado que el 65.00% de los trabajadores y clientes SI consideran importante una seguridad informática honeypot, mientras que un 35.00% afirma que NO. Mi aporte es determinar si es importante ya que de esa manera se está contribuyendo a que se termine con la ciberdelincuencia que se vive en estos tiempos y pone en riesgo la información valiosa de todas las personas. Como valor agregado en esta investigación, la importancia de contar con un honeypot ayuda a mejorar nuestra seguridad informática.

2. Se determinó con respecto al nivel de necesidad para la implementación de un honeypot, que el 80.00% de los trabajadores y clientes SI consideran necesario la implementación de un honeypot, mientras que un 20.00% afirma que NO. Mi aporte es estudiar la necesidad de implementación de un honeypot con el objetivo de mejorar la seguridad informática para resguardar la información valiosa de la Agropecuaria Wilian & Roque S.R.L. Como valor agregado es determinar cuales fueron esas necesidades que permite hacer la instalación del honeypot.

3. Con la utilización de la metodología PPDIOO de cisco nos permitió un mejor manejo de todo esto y desarrollar de buena manera que todos los procesos se trabajen de manera ordenada con cada de una de sus fases para desarrollar mi propuesta. Mi aporte consistió en usar la metodología PPDIOO para desarrollar cada fase se terminen con la última fase y no haiga ninguna confusión con el desarrollo. Como valor agregado en esta investigación, la metodología usada ayuda a mejorar la realización de nuestro proyecto de la mejor manera.

4. Se realizó la simulación de un honeypot dentro de VirtualBox para manejar los ataques cibernéticos, permitiendo así observar los problemas que se viene dando ante la ciberdelincuencia y por ende prevenir futuros ataques. Mi aporte consiste en realizar el honeypot mediante una simulación con la finalidad de ver las interacciones. Como valor agregado de la investigación, la simulación realizada ayuda a controlar los ataques cibernéticos.

RECOMENDACIONES

Según lo propuesto para la implementación de un honeypot de seguridad informática en la Agropecuaria Wilian & Roque S.R.L., con la finalidad de controlar los ataques cibernéticos:

1. Se sugiere tomar en cuenta realizar un presupuesto para la instalación del honeypot dentro de las redes de la empresa, para combatir con los ciberdelincuentes que quieren robarnos la información de la empresa.

2. Se sugiere usar la metodología PPDIOO planteada, para la realización de una futura instalación de un honeypot dentro de la empresa, que les ayudará a tener un mejor entendimiento de lo que se hará y tener las cosas más claras.

3. Se recomienda realizar cada cierto tiempo mantenimiento del honeypot para visualizar posibles problemas que puedan suceder.

4. Se recomienda realizar la implementación a un corto tiempo ya que la seguridad informática de la empresa corre el peligro de ser vulnerado por ciberdelincuentes.

REFERENCIAS BIBLIOGRÁFICAS

1. Giant N. Ciberseguridad para la i-generación : usos y riesgos de las redes sociales y sus aplicaciones. Narcea Ediciones, editor. Madrid; 2017. 1-160 p.

2. Hernández L, Lerma C. Aplicaciones Prácticas de los Honeypots en la Protección y Monitoreo de Redes de Información. CienciaUAT [Internet]. 2007 [citado 6 de junio de 2019];1(4):8-12. Disponible en: http://www.redalyc.org/articulo.oa?id=441942908009

3. Florez I, Quintana J. Sistema de Detección de Ataques Informáticos a Redes de Datos Empresariales Soportado en Honeypots [Internet] [Tesis]. [Cartagena de Indias]: Universidad de Cartagena; 2018 [citado 5 de mayo de 2020]. Disponible en: http://repositorio.unicartagena.edu.co/bitstream/handle/11227/8498/TESIS FLOREZ- MANQUINTANA.pdf?sequence=1&isAllowed=y

4. Rodríguez E. Estudio y desarrollo de la automatización de una red de sensores global de honeypots [Internet]. Universidad Autonoma De Madrid; 2017 [citado 1 de junio de 2019]. Disponible en: https://repositorio.uam.es/handle/10486/680054

5. Matus J. Analisis e implementación de una solucion honeypot para un entorno experimental [Tesis]. [Mexico]: Universidad de quintana roo; 2017.

6. Ochoa A. Diseño de una Red de Seguridad Informatica para la Protección de Sistema Web de un Call Center ante Ataques Informaticos Aplicando la Norma iso 27033 [Tesis]. [Lima]: Universidad peruana de ciencias aplicadas; 2019.

7. Romero K. Propuesta de seguridad informática para mejorar el proceso de acceso remoto en una entidad financiera [Tesis]. [Lima]: Universidad san ignacio de loyola; 2018.

8. Pomalaya K. Rediseño de la red de datos para mejorar la seguridad informatica de una municipalidad [Tesis]. [Huancayo]: Universidad peruana los andes; 2018.

9. Llerena R. Evaluación de la seguridad informática en el área de sistemas de la municipalidad distrital de nuevo chimbote [Tesis]. [Chimbote]: Universidad san pedro; 2018.

10. De la Cruz F. Aplicación de metodologías y herramientas de la informática forense para reducir el riesgo de la seguridad informática en la dirección nacional de comunicación y criminalística de la policía nacional del Perú – Huaraz - 2015 [Internet] [Tesis]. [Huaraz]: Universidad Nacional Santiago Antúnez de Mayolo; 2017 [citado 1 de junio de 2019]. Disponible en: http://repositorio.unasam.edu.pe/handle/UNASAM/2626

11. Alvarado J. Análisis de las vulnerabilidades mediante el uso de phishing para mejorar la seguridad informática de los equipos de cómputo y redes de la municipalidad distrital de Independencia [Internet] [Tesis]. Universidad Nacional Santiago Antúnez de Mayolo. [Huaraz]: Universidad Nacional Santiago Antúnez de Mayolo; 2017 [citado 1 de junio de 2019]. Disponible en: http://repositorio.unasam.edu.pe/handle/UNASAM/2655

12. Villanueva R. Agropecuaria Wilian & Roque S.R.L. | Agricola Serrano [Internet]. [citado 26 de octubre de 2020]. Disponible en: https://www.universidadperu.com/empresas/agropecuaria-wilian-roque.php

13. Agropecuaria Wilian & Roque - 859 Jirón Francisco Pizarro - Google Maps [Internet]. [citado 4 de junio de 2021]. Disponible en: https://www.google.com/maps/place/Jirón+Francisco+Pizarro+859,+Chimbote+02802/@-9.071174,-78.5881695,3a,75y,46.56h,93.5t/data=!3m7!1e1!3m5!1shAnHfNnTeFAjOlsDvrmD6w!2e0!6shttps:%2F%2Fstreetviewpixels-pa.googleapis.com%2Fv1%2Fthumbnail%3Fpanoid%3DhAnHfNnTeFAjOlsDvrmD6w%26cb_client%3Dsearch.gws-prod.gps%26w%3D86%26h%3D86%26yaw%3D22.56477%26pitch%3D0%26thumbfov%3D100!7i13312!8i6656!4m5!3m4!1s0x91ab813e07edd8f1:0xb7c6b8ad07dc6987!8m2!3d-9.0710774!4d-78.5881525

14. Lener. Las tecnologías de información en las empresas - Evaluando Software

[Internet]. 2021 [citado 11 de mayo de 2020]. Disponible en: https://www.evaluandosoftware.com/las-tecnologias-de-informacion-y-comunicaciones-en-las-empresas/

15. Barreto C, Díazgranados F, Hung E, Cantillo B, Molinares D, Salcedo E, et al. Las TIC en educación superior : experiencias de innovación. Universida. 2017.

16. Montano J. Historia de las TICs: desde su Origen Hasta la Actualidad - Lifeder [Internet]. Lifeder.com. 2019 [citado 5 de mayo de 2020]. Disponible en: https://www.lifeder.com/historia-tics/

17. Meléndez J. DELITOS INFORMÁTICOS O CIBERDELITOS - Derecho Ecuador - [Internet]. 2020 [citado 11 de mayo de 2020]. Disponible en: https://www.derechoecuador.com/delitos-informaticos-o-ciberdelitos

18. Dominguez J. Seguridad Informática Personal y Corporativa (Segunda parte) [Internet]. IEASS. Editores, editor. Venezuela; 2017 [citado 11 de mayo de 2020]. Disponible en: https://www.researchgate.net/publication/286371326_Seguridad_Informatica_Personal_y_Corporativa_Segunda_parte

19. Rodríguez E. ¿Qué es un honeypot y cómo usarlo en beneficio de tu negocio? [Internet]. GoDaddy. 2019 [citado 5 de mayo de 2020]. Disponible en: https://es.godaddy.com/blog/que-es-un-honeypot-y-como-usarlo-en-beneficio-de-tu-negocio/

20. Fruhlinger J. ¿Qué es un honeypot? Una trampa para atrapar a los hackers en el acto | CambioDigital OnLine [Internet]. Cambio Digital. 2019 [citado 5 de mayo de 2020]. Disponible en: https://cambiodigital-ol.com/2019/04/que-es- un-honeypot-una-trampa-para-atrapar-a-los-hackers-en-el-acto/

21. Bazo U. ¿Qué es un honeypot? Una trampa para atrapar a los hackers en el acto [Internet]. 2019 [citado 11 de mayo de 2020]. Disponible en: https://cioperu.pe/articulo/27862/que-es-un-honeypot-una-trampa-para-atrapar-a-los-hackers-en-el/

22. Olano J. Honeypots; descubre qué son, monitorízalos y caza al cazador [Internet]. Pandorafms. 2017 [citado 5 de mayo de 2020]. Disponible en: https://pandorafms.com/blog/es/honey-pots/

23. Navarrete G. «HoneyBot»: el robot creado para combatir a los hackers - La Tercera [Internet]. 2018 [citado 11 de mayo de 2020]. Disponible en: https://www.latercera.com/la-tercera-tv/noticia/honeybot-robot-creado-combatir-los-hackers/122012/

24. Sanchez I. Explicación de Honeypot e instalación de kippo y kippo-graph. – Hardsoft Security [Internet]. 2018 [citado 11 de mayo de 2020]. Disponible en: https://hardsoftsecurity.es/index.php/2018/06/25/explicacion-de-honeypot-e-instalacion-de-kippo-y-kippo-graph/

25. Bustos L. Honeypots [Internet]. 2017 [citado 11 de mayo de 2020]. Disponible en: https://prezi.com/rdtsat0bhdbf/honeypots/

26. Verdejo G. Capitulo 4: Seguridad en redes ip:Honeypots y honeynets [Internet]. 2018 [citado 5 de mayo de 2020]. Disponible en: https://www.cs.upc.edu/~gabriel/files/DEA-es-4HoneypotsyHoneynets.pdf

27. Ferrer M. Firewalls Software: Estudio, instalación, configuración de escenarios y comparativa [Internet]. [España]: Universitat Politécnica de Catalunya; 2006 [citado 19 de octubre de 2020]. Disponible en: https://upcommons.upc.edu/bitstream/handle/2099.1/3756/54344-2.pdf?sequence=2&isAllowed=y

28. Cobo A, Gómez P, Pérez D, Rocha R. PHP y MySQL: Tecnología para el desarrollo de aplicaciones web [Internet]. Ediciones Diaz de Santos, editor. España; 2005. Disponible en: https://books.google.es/books?hl=es&lr=&id=zMK3GOMOpQ4C&oi=fnd&pg=PR17&dq=mysql+definiciones&ots=FhftY-G9nk&sig=PUofm5LRY5QG8rVqPWR93enkiBE#v=onepage&q=mysql definiciones&f=false

29. López P. Cómo usar VirtualBox para crear una máquina virtual [Internet]. 2019 [citado 25 de octubre de 2020]. Disponible en: https://www.geeknetic.es/Noticia/17411/Como-usar-VirtualBox-para-crear-una-maquina-virtual.html

30. Lagla C. Propuesta de rediseño de red de datos de la empresa cobrafacil fabrasilisa s.a bajo metodología ppdioo y de diseño top-down [Internet]. [Quito]: Universidad politécnica salesiana sede quito; 2019 [citado 4 de junio de 2021]. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/16686/1/UPS-ST003882.pdf

31. Cueva T, Mishahuaman X. Metodología top down network design para elevar la eficiencia de la red de datos en la Municipalidad Provincial de Huánuco – 2019 [Internet]. [Huánuco]: Universidad Nacional Hermilio Valdizán; 2019 [citado 30 de julio de 2022]. Disponible en: https://repositorio.unheval.edu.pe/handle/20.500.13080/5525

32. Hernández L, Fernández R, Baptista P. Metodología de la investigación [Internet]. Sexta Edic. McGraw-Hill / Interamericana Editores SADCV, editor. México; 2014 [citado 9 de mayo de 2020]. 1-632 p. Disponible en: https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

33. Sánchez H, Reyes C, Mejía K. Manual de términos en investigación científica, tecnológica y humanística. Primera Ed. Palma UR, editor. Lima - Perú: Universidad Ricardo Palma; 2018. 1323-1330 p.

34. Tamayo M. El proceso de la investigación científica. Cuarta Edi. Editorial Limusa SA de CVGNE, editor. Mexico; 2003.

35. Hn.pe. ¿Qué son los ataques informáticos? | hn.pe [Internet]. Hostname. 2017 [citado 11 de mayo de 2020]. Disponible en: https://www.hn.pe/blog/que-son-los-ataques-informaticos

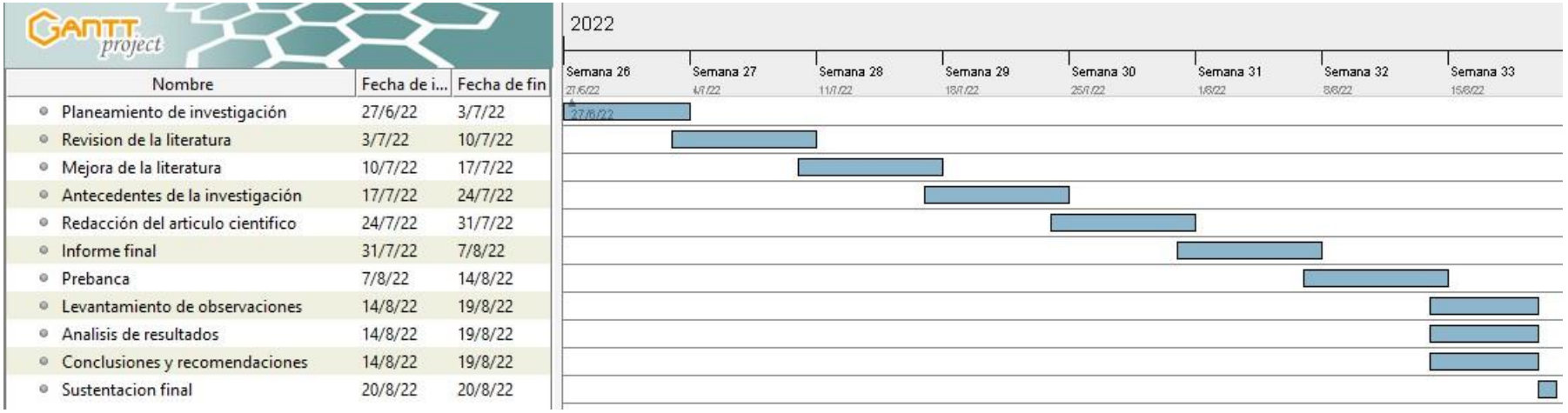
36. López P, Fachelli S. Metodología De La Investigación Social Cuantitativa. Edición Di. Deposito Digital De Documentos UAB, editor. Barcelona: Universidad Autónoma De Barcelona; 2015.

37. Rectorado. Código de ética para la investigación.Versión 002.Comité Institucional de Ética en Investigación. Univ Católica los Angeles Chimbote [Internet]. 2019;1-7. Disponible en: https://www.uladech.edu.pe/images/stories/universidad/documentos/2019/codigo-de-etica-para-la-investigacion-v002.pdf

38. Rectorado. Reglamento de investigacion v017 [Internet]. Univ Católica los Angeles Chimbote; [citado 4 de junio de 2021]. Disponible en: https://www.uladech.edu.pe/images/stories/universidad/documentos/2020/reglamento_investigacion_v015.pdf

ANEXOS

ANEXO NRO. 1: CRONOGRAMA DE ACTIVIDADES



Nombre	Fecha de i...	Fecha de fin
Planeamiento de investigación	27/6/22	3/7/22
Revision de la literatura	3/7/22	10/7/22
Mejora de la literatura	10/7/22	17/7/22
Antecedentes de la investigación	17/7/22	24/7/22
Redacción del articulo cientifico	24/7/22	31/7/22
Informe final	31/7/22	7/8/22
Prebanca	7/8/22	14/8/22
Levantamiento de observaciones	14/8/22	19/8/22
Analisis de resultados	14/8/22	19/8/22
Conclusiones y recomendaciones	14/8/22	19/8/22
Sustentacion final	20/8/22	20/8/22

Fuente: Elaboración propia.

ANEXO NRO. 2: PRESUPUESTO Y FINANCIAMIENTO

TÍTULO: Propuesta de implementación de un honeypot de seguridad informática en la agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

ESTUDIANTE: Terrones Bedón Víctor Manuel

INVERSIÓN: S/. 780.17

FINANCIAMIENTO: RECURSOS PROPIOS

Tabla Nro. 33: Presupuesto y financiamiento

Presupuesto desembolsable (Estudiante)			
Categoria	Base	% o numero	Total (s/.)
Suministros(*)			
•Impresiones	0.20	20	14.00
•Fotocopias	0.10	30	3.00
•Espiralado	9.00	3	27
•Papel bond A-4 (500 hojas)	15.00	500	7.17
•Lapiceros	1.00	2	2.00
Servicios			
•Uso de Turnitin	50.00	1	50.00
Sub Total			
Gastos de viaje			
•Pasajes para recolectar información	5.00	5	25.00
Sub total			128.17
Total de presupuesto desembolsable			
Presupuesto no desembolsble (Universidad)			
Categoria	Base	% o numero	TOTAL (s/.)
Servicios			
•Uso de internet (Laboratorio de Aprendizaje Digital-LAD)	30.00	4	120.00
•Búsqueda de información en base de datos	35.00	2	70.00
•Soporte informático (Modulo de Investigación del ERP University-MOIC)	40.00	4	160.00
•Publicación de artículo en repositorio institucional	50.00	1	50.00
Sub total			
Recurso humano			
•Asesoría personalizada (5 horas por semana)	63.00	4	252.00
Sub total			252.00
Total de presupuesto no desembolsable			652.00
Total(S/.)			

Fuente: Reglamento de investigación V017 (38).

ANEXO NRO. 3: CUESTIONARIO

TÍTULO: PROPUESTA DE IMPLEMENTACIÓN DE UN HONEYPOT DE SEGURIDAD INFORMÁTICA EN LA AGROPECUARIA WILIAN & ROQUE S.R.L. – CHIMBOTE; 2021.

AUTOR: TERRONES BEDÓN VICTOR MANUEL

PRESENTACIÓN:

El presente instrumento forma parte del actual trabajo de investigación; por lo que se solicita su participación, respondiendo a cada pregunta de manera objetiva y veraz. La información a proporcionar es de carácter confidencial y reservado; y los resultados de la misma serán utilizados solo para efectos académicos y de investigación científica.

INSTRUCCIONES:

A continuación, se le presenta una lista de preguntas, agrupadas por dimensión, que se solicita se responda, marcando una sola alternativa con un aspa ("X") en el recuadro correspondiente (SI o NO) según considere su alternativa:

Tabla Nro. 34: Cuestionario

DIMENSIÓN 1: NIVEL DE IMPORTANCIA DE UNA SEGURIDAD INFORMATICA HONEYPOT			
NRO.	**PREGUNTA**	**SI**	**NO**
1	¿Considera importante que la Agropecuaria Wilian & Roque S.R.L. cuente con un software de seguridad informática?		
2	¿Conoce usted sobre una herramienta honeypot para la seguridad informática en una empresa?		
3	¿Piensa usted que un honeypot podría terminar con los peligros cibernéticos que vulneran los sistemas de la empresa?		
4	¿Cree usted importante que las personas hoy en día deban conocer y utilizar un honeypot como seguridad en sus negocios?		

5	¿Considera que el análisis de un honeypot ayude a mantener la seguridad de sus datos en la empresa?		
6	¿Conoce o a escuchado sobre alguna empresa que ha sufrido de robos o amenazas en sus sistemas?		
7	¿Cree que un honeypot traería mucha ventaja para la Agropecuaria Wilian & Roque S.R.L.?		
8	¿Usted conoce de qué forma puede ser atacado un sistema?		
9	¿Conoce usted que resultados o consecuencias puede traer los ataques cibernéticos?		
10	¿Consideras que los ataques cibernéticos son una amenaza para el desarrollo de una empresa?		

Fuente: Elaboración Propia

DIMENSIÓN 2: NIVEL DE NECESIDAD PARA IMPLEMENTAR UN HONEYPOT			
NRO.	**PREGUNTA**	**SI**	**NO**
1	¿Cree usted que sería beneficioso implementar un honeypot en la empresa?		
2	¿Considera importante que los datos de la empresa mantengan una estabilidad y seguridad?		
3	¿Cree que el desarrollo de la implementación de un software de seguridad informática reduciría las vulnerabilidades que mantiene algunas empresas?		
4	¿Sera importante que hoy en día las empresas implementen una seguridad para sus sistemas como un honeypot?		
5	¿Conoce usted de algún problema que ha mantenido la empresa sobre una pérdida de información?		
6	¿Considera importante que hoy en día con la implementación de un honeypot no habría pérdidas económicas?		
7	¿Cree usted que el avance de la tecnología está haciendo que los ataques cibernéticos crezcan?		
8	¿Considera que la Agropecuaria Wilian & Roque S.R.L. debería dedicarse no solo en ventas sino en mantener seguro su información?		
9	¿Considera que la implementación de un honeypot sea beneficioso para la empresa y sus clientes?		
10	¿Cree usted que la empresa mantenga una seguridad estable y conforme con sus sistemas hoy en día?		

Fuente: Elaboración propia

ANEXO NRO. 4: FICHAS DE VALIDACIÓN

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Nombres y apellidos del validador : MARTIN GUSTAVO SALCEDO QUIÑONES
1.2 Cargo e institución donde labora : DOCENTE TUTOR - CHIMBOTE - ULADECH
1.3 Nombre del instrumento evaluado : CUESTIONARIO
1.4 Autor del instrumento : TERRONES BEDON VICTOR MANUEL

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según la calificación que asigna a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador).
2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador).
3. Buena (Si más del 70% de los ítems cumplen con el indicador).

Aspectos de validación del instrumento		1	2	3	Observaciones
Criterios	Indicadores	D	R	B	Sugerencias
• PERTINENCIA	Los ítems miden lo previsto en los objetivos de investigación.	☐	☐	☒	
• COHERENCIA	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.	☐	☐	☒	
• CONGRUENCIA	Los ítems son congruentes entre sí y con el concepto que mide.	☐	☐	☒	
• SUFICIENCIA	Los ítems son suficientes en cantidad para medir la variable.	☐	☐	☒	
• OBJETIVIDAD	Los ítems se expresan en comportamientos y acciones observables.	☐	☐	☒	
• CONSISTENCIA	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.	☐	☐	☒	
• ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.	☐	☒	☐	
• CLARIDAD	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar.	☐	☐	☒	
• FORMATO	Los ítems están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	☐	☐	☒	
• ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuesta bien definidas.	☐	☐	☒	
CONTEO TOTAL (Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador)		C	B	A	Total

Coeficiente de validez : $\frac{A+B+C}{30} = \frac{27+2+0}{30} = 0,97$

Intervalos	Resultado
0,00 – 0,49	• Validez nula
0,50 – 0,59	• Validez muy baja
0,60 – 0,69	• Validez baja
0,70 – 0,79	• Validez aceptable
0,80 – 0,89	• Validez buena
0,90 – 1,00	• Validez muy buena

III. CALIFICACIÓN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

Validez muy buena

Ing. Martín G. Salcedo Quiñones
CIP. 88711

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Nombres y apellidos del validador : Edgard Vilcarino Zelada

1.2 Cargo e institución donde labora Docente Uladech

1.3 Nombre del instrumento evaluado : Cuestionario

1.4 Autor del instrumento Viciar Manuel Terrones Bedón

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según la calificación que asigna a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador).
2. Regular (Si entre el 31 % y 70% de los ítems cumplen con el indicador).
3. Buena (Sí más del 70% de los ítems cumplen con el indicador).

Asoectosde validaciórdel instrumento		1	2	3	Observaciones
Criterios	**Indicadores**	**D**	**R**	**B**	**Sugerencias**
• PERTINENCIA	Los ítems miden lo previsto en los objetivos de investigación.	O	O	x O	
• COHERENCIA	Los iterns responden a lo que se debe medir en la variable y sus dimensiones.	O	O	x O	
• CONGRUENCIA	Los ítems son congruentes entre si y con el concepto que mide.	O	x O	O	
• SUFICIENCIA	Los íterns son suficientes en cantidad para medir la variable.	O	x O	O	
• OBJETIVIDAD	Los ítems se expresan en comportamientos y acciones observables.	O	x O	O	
• CONSISTENCIA	Los items se han formulado en concordancia a los fundamentos teóricos de la variable.	O	O	x O	
• ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.	O	O	x O	
• CLARIDAD	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar.	O	x O	O	
• FORMATO	Los items están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	O	O	x O	
• ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuesta bien definidas.	O	O	x O	
	CONTEO TOTAL (Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador)		**4**	**6**	
		e	**B**	**A**	**Total**

:oeficiente e validez: $\frac{A+B+C}{30} = \mathbf{0.86}$

Intervalos	Resultado
0.00–0,49	• Validez nula
0.50–0,59	• Validez mu ba a
0,60–0,69	ja
0,70–0,79	• Validez aceptable
0,80–0,89	• Validez buena
0,90-1,00	y a

III. CALIFICACIÓN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado

Validez buena

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Nombres y apellidos del validador : Noé Gregario Silva Zelada

1.2 Cargo e institución donde labora Magíster en Docencia Universitaria

1.3 Nombre del instrumento evaluado : Cuestionario

1.4 Autor del instrumento Terrones Bedón Víctor Manuel

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según la calificación que asigna a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador).
2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador).
3. Buena (Si más del 70% de los ítems cumplen con el indicador).

Asoectos de validación del instrumento		1	2	3	Observaciones
Criterios	Indicadores	0	R	B	Sugerencias
• PERTINENCIA	Los ítems miden lo previsto en los objetivos de investigación.	D	D	x D	
• COHERENCIA	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.	D	D	x D	
• CONGRUENCIA	Los ítems son congruentes entre si y con el concepto que mide.	D	D	x D	
• SUFICIENCIA	Los ítems son suficientes en cantidad para medir la variable.	D	D	x D	
• OBJETIVIDAO	Los items se expresan en comportamientos y acciones observables.	D	D	x D	
• CONSISTENCIA	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.	D	D	x D	
• ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.	D	x D	D	
• CLARIDAO	Los items están redactados en un lenguaje entendible para los sujetos a evaluar.	D	D	x D	
• FORMATO	Los items están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	D	D	x D	
• ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuesta bien definidas.	D	D	x D	

CONTEO TOTAL

(Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador)

e B A Total

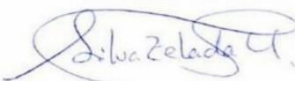
Coeficiente de validez : $\frac{A+B+C}{30} = \frac{0.97}{}$

Intervalos	Resultado
0.00–0.49	• Validez nula
0.50–0 59	• Validez muy baja
	• Validez baja
	• Validez aceptable
	• Validez buena
	• Validez muy buena

III. CALIFICACIÓN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

Muy Buena



Mgtr. Noé Gregario Silva Zelada

CIP: 83347

ANEXO NRO. 5: CONSENTIMIENTO INFORMADO

Investigador principal del proyecto: TERRONES BEDÓN, VICTOR MANUEL

Consentimiento informado

Estimado participante, Villanueva Rosales Rolando Guillermo.

El presente estudio tiene como objetivo: Realizar la propuesta de implementación de un honeypot de seguridad informática en la Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2020, con la finalidad de controlar los ataques cibernéticos.

La presente investigación se informa acerca de la Agropecuaria Wilian & Roque S.R.L. en cual se encarga de venta de fertilizantes entre otros productos, además de manejar correos que envían a sus clientes, ya que toda esta información que maneja puede ser atacada por ciberdelincuentes, se busca controlar los ataques cibernéticos.

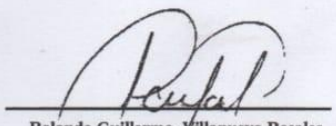
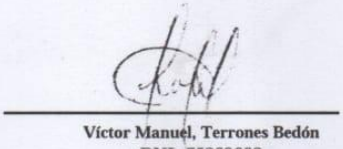
Toda la información que se obtenga de todos los análisis será confidencial y sólo los investigadores y el comité de ética podrán tener acceso a esta información. Será guardada en una base de datos protegidas con contraseñas. Tu nombre no será utilizado en ningún informe. Si decides no participar, no se te tratará de forma distinta ni habrá prejuicio alguno. Si decides participar, eres libre de retirarse del estudio en cualquier momento.

Si tienes dudas sobre el estudio, puedes comunicarte con el investigador principal de Chimbote, Perú VICTOR MANUEL TERRONES BEDÓN al celular: 930460083, o al correo: victor_17_1998@hotmail.com.

Si tienes dudas acerca de tus derechos como participante de un estudio de investigación, puedes llamar a la Mg. Zoila Rosa Limay Herrera presidente del Comité institucional de Ética en Investigación de la Universidad Católica los Ángeles de Chimbote, Cel: (+51043) 327-933, Email: zlimayh@uladech.edu.pe

Obtención del Consentimiento Informado

Me ha sido leído el procedimiento de este estudio y estoy completamente informado de los objetivos del estudio. El (la) investigador(a) me ha explicado el estudio y absuelto mis dudas. Voluntariamente doy mi consentimiento para participar en este estudio:

PARTICIPANTE	ENCUESTADOR
	
Rolando Guillermo, Villanueva Rosales	**Víctor Manuel, Terrones Bedón**
DNI: 33256996	**DNI: 75269602**