ANEXO 1

FORMATO PARA LA PRESENTACIÓN DE PROYECTOS DE INVESTIGACIÓN CON EL FINANCIAMIENTO DEL FEDU

**1.** Título del proyecto

| |
|---|
| **Intrusion Detection and Prevention System for Production Supervision in Small Businesses Based on Raspberry Pi and Snort** |

2. Área de Investigación

| Área de investigación | Línea de Investigación | Disciplina OCDE |
|---|---|---|
| **SISTEMAS COMPUTACIÓN E INFORMÁTICA** | **TELECOMUNICACIONES Y REDES DE DATOS** | **TELECOMUNICACIONES** |

3. Duración del proyecto (meses)

| |
|---|
| **12** |

4. Tipo de proyecto

| | |
|---|---|
| Individual | ● |
| Multidisciplinario | ○ |
| Director de tesis pregrado | ○ |

4. Datos de los integrantes del proyecto

| | |
|---|---|
| **Apellidos y Nombres** | **Cruz de la Cruz José Emmanuel** |
| **Escuela Profesional** | **Ingeniería Electrónica** |
| **Celular** | **951 175 865** |
| **Correo Electrónico** | **jeccruz@yahoo.com** |

**I.** Título (El proyecto de tesis debe llevar un título que exprese en forma sintética su contenido, haciendo referencia en lo posible, al resultado final que se pretende lograr. Máx. palabras 25)

| |
|---|
| Intrusion Detection and Prevention System for Production Supervision in Small Businesses Based on Raspberry Pi and Snort |

**II.** Resumen del Proyecto de Tesis (Debe ser suficientemente informativo, presentando -igual que un trabajo científico- una descripción de los principales puntos que se abordarán, objetivos, metodología y resultados que se esperan**)**

| |
|---|
| A computer security system is a set of processes that are highly dependent on information technology (IT) personnel focused on cyber security, as companies can become victims of hackers and cyber criminals, thus losing the trust of the environment of production, telecommuting and consequently also losing business confidence. A cyber analyst is very important in the staff of any company, since |

he will implement security solutions, however, the collaboration of one of these specialists in a small company is an additional cost in terms of staff salary and in the acquisition of tools it needs. It is for this reason that the development of an intrusion detection and prevention system begins, which will not require a greater investment in the budget of small companies, this being a solid security stack that allows registration, visibility and automatic response to Possible threats on the network, of course, can be remotely managed and analyzed by a specialist, the annual cost of the full service is approximately $209 USD. The system is based on Raspberry Pi hardware and free Ubuntu Server software as the operating system and Snort as the intrusion detection and prevention system.

**III.** Palabras claves (Keywords) (Colocadas en orden de importancia. Máx. palabras: cinco**)**

ids, ips, snort, raspberry pi, small business, telework, security, ubuntu server.

**IV.** Justificación del proyecto (Describa el problema y su relevancia como objeto de investigación. Es importante una clara definición y delimitación del problema que abordará la investigación, ya que temas cuya definición es difusa o amplísima son difíciles de evaluar y desarrollar**)**

The need to guarantee the safety of users as well as the protection of company data, means that you have to invest in professionals who are experts in cybercrime, cyber analysts, etc. to ensure the trust of their workers when carrying out different types of collaboration within small companies that have low budgets, so these practices are almost non-existent or they hire developers who are responsible for both, software development and system security deployment, which is a very bad practice for any business environment.

Snort IDS was tested on a multi-purpose and low-cost computer called Raspberry Pi, with a specific objective of determining their performance, efficiency and efficacy for use in computer network environments, where cost is a determining factor.

**V.** Antecedentes del proyecto (Incluya el estado actual del conocimiento en el ámbito nacional e internacional. La revisión bibliográfica debe incluir en lo posible artículos científicos actuales, para evidenciar el conocimiento existente y el aporte de la Tesis propuesta. Esto es importante para el futuro artículo que resultará como producto de este trabajo)

A. Kar Kyaw, Y. Chen and J. Joseph, "Pi-IDS: evaluation of open-source intrusion detection systems on Raspberry Pi 2," IEEE Xplore, 2015.

A. Sforzin, F. Gómez Mármol, M. Conti and J.-M. Bohli, "RPiDS: Raspberry Pi IDS - A Fruitful Intrusion Detection System for IoT," IEEE Xplore, 2017.

M. Cosar and H. E. Kiran, "Performance Comparison of Open Source IDSs via Raspberry Pi," IEEE Xplore, 2019.

M. Cosar and S. Karasartova, "A firewall application on SOHO networks with Raspberry Pi and snort," IEEE Xplore, 2017.

R. Gaddam and M. Nandhini, "An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment," IEEE Xplore, 2017.

P. Patil and A. Kokil, "WiFiPi-Tracking at mass events," IEEE Xplore, 2015.

V. Vujović, M. Maksimović, B. Perišić and G. Milošević, "A proposition of low cost Sensor Web

implementation based on GSM/GPRS services," IEEE Xplore, 2017.
E. Al Neyadi, S. Al Shehhi, A. Al Shehhi, N. Al Hashimi, M. Qbea'H and S. Alrabaee, "Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux," IEEE Xplore, 2020.

## VI. Hipótesis del trabajo (Es el aporte proyectado de la investigación en la solución del problema)

In particular, we evaluated the performance of the Raspberry Pi, one of the most used commodity single-board computers, while running Snort, a widely known, open source IDS

## VII. Objetivo general

In Small Office/Home Office (SOHO) computer networks, an IDS can be activated to intercept the possible attack. Open source code IDS such as snort and strata can be used together with Raspberry Pi computers

## VIII. Objetivos específicos

Security and reliability are the major concern of our daily life usage of any network. But with the swift advancements in network technology, attacks are becoming more sophisticated than defenses. Using popular open source software Snort as IDS tool, can be easily configured and deployed in any environment

## IX. Metodología de investigación (Describir el(los) método(s) científico(s) que se empleará(n) para alcanzar los objetivos específicos, en forma coherente a la hipótesis de la investigación. Sustentar, con base bibliográfica, la pertinencia del(los) método(s) en términos de la representatividad de la muestra y de los resultados que se esperan alcanzar. Incluir los análisis estadísticos a utilizar**)**

The need to guarantee the safety of users as well as the protection of company data, means that you have to invest in professionals who are experts in cybercrime, cyber analysts, etc. to ensure the trust of their workers when carrying out different types of collaboration within small companies that have low budgets, so these practices are almost non-existent or they hire developers who are responsible for both, software development and system security deployment, which is a very bad practice for any business environment.

Snort IDS was tested on a multi-purpose and low-cost computer called Raspberry Pi, with a specific objective of determining their performance, efficiency and efficacy for use in computer network environments, where cost is a determining factor.

## X. Referencias (Listar las citas bibliográficas con el estilo adecuado a su especialidad)

A. Kar Kyaw, Y. Chen and J. Joseph, "Pi-IDS: evaluation of open-source intrusion detection systems on Raspberry Pi 2," IEEE Xplore, 2015.
A. Sforzin, F. Gómez Mármol, M. Conti and J.-M. Bohli, "RPiDS: Raspberry Pi IDS - A Fruitful Intrusion Detection System for IoT," IEEE Xplore, 2017.
M. Cosar and H. E. Kiran, "Performance Comparison of Open Source IDSs via Raspberry Pi," IEEE Xplore, 2019.
M. Cosar and S. Karasartova, "A firewall application on SOHO networks with Raspberry Pi and snort," IEEE Xplore, 2017.

R. Gaddam and M. Nandhini, "An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment," IEEE Xplore, 2017.
P. Patil and A. Kokil, "WiFiPi-Tracking at mass events," IEEE Xplore, 2015.
V. Vujović, M. Maksimović, B. Perišić and G. Milošević, "A proposition of low cost Sensor Web implementation based on GSM/GPRS services," IEEE Xplore, 2017.
E. Al Neyadi, S. Al Shehhi, A. Al Shehhi, N. Al Hashimi, M. Qbea'H and S. Alrabaee, "Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux," IEEE Xplore, 2020.

## XI. Uso de los resultados y contribuciones del proyecto (Señalar el posible uso de los resultados y la contribución de los mismos)

Networking Security

## XII. Impactos esperados

### i. Impactos en Ciencia y Tecnología

New methodology for networking security

### ii. Impactos económicos

Savings in equipment costs

### iii. Impactos sociales

Security

### iv. Impactos ambientales

Green equipment

## XIII. Recursos necesarios (Infraestructura, equipos y principales tecnologías en uso relacionadas con la temática del proyecto, señale medios y recursos para realizar el proyecto)

Raspberry Pi 3 B, its cost is $43 USD.
The interesting hardware for this research is mainly made up of:

- Quad Core 1.2GHz Broadcom BCM2837 64bit CPU.
- 1GB RAM.
- BCM43438 wireless LAN.
- 100 Base Ethernet.
- 40-pin extended GPIO.
- 4 USB 2 ports.
- Full size HDMI.
- Micro SD port for loading your operating system and storing data.
- Upgraded switched Micro USB power source up to 2.5A.

**XIV.** Localización del proyecto (indicar donde se llevará a cabo el proyecto)

Puno, Perú

**XV.** Cronograma de actividades

| Actividad | Trimestres | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | E | F | M | A | M | J | J | A | S | O | N | D |
| References review | X | X | X | | | | | | | | | |
| Methodoly design | | | | X | X | X | | | | | | |
| Results | | | | | | | X | X | X | | | |
| Conclusions | | | | | | | | | | X | X | X |

**XVI.** Presupuesto

| Descripción | Unidad de medida | Costo Unitario (S/.) | Cantidad | Costo total (S/.) |
|---|---|---|---|---|
| Raspberry Pi 3 B | UND | 180 | 1 | 180 |
| | | | | |
| | | | | |