UNIVERSIDAD NACIONAL DE UCAYALI

ESCUELA DE POSGRADO

LOS SISTEMAS DE CIFRADO ROCE EN LA SEGURIDAD DE ARCHIVOS DE TEXTO

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN CIENCIAS DE LA COMPUTACION

TESISTA
YUMI TOMINAGA GARCIA

PUCALLPA – PERÚ
2021

UNIVERSIDAD NACIONAL DE UCAYALI
ESCUELA DE POSGRADO

ANEXO Nº 4

ACTA DE DEFENSA DE TESIS O TRABAJO DE INVESTIGACION PARA OBTENCION DEL GRADO DE MAESTRO O MAESTRO EN CIENCIAS

En la Sala de Grados de la Universidad Nacional de Ucayali siendo las 10:00 a.m. horas, del día 12 de marzo del 2021, ante el **Jurado** de Tesis o trabajo de investigación constituido por :

Mg. ROMEL PINEDO RIOS.	Presidente
Mg. ARTURO YUPANQUI VILLANUEVA	Secretario
Mg. CLOTILDE HIDALGO DE CERNA	Vocal

El aspirante al **GRADO DE MAESTRO O MAESTRO EN CIENCIA DE LA COMPUTACIÓN**.....Mención: .....

Don (ña) **Sr. YUMI TOMINAGA GARCIA**.

Procedió al acto de Defensa:

a. Con la exposición de la tesis o trabajo de investigación, titulada:

"LOS SISTEMAS DE CIFRADO ROCE EN LA SEGURIDAD DE ARCHIVOS DE TEXTO".

b. Respondiendo las preguntas formuladas por los miembros del Jurado y público asistente.

Concluido el acto de defensa, cada miembro del Jurado procedió a la evaluación del aspirante a Maestro, teniendo presente los criterios siguientes:

a) Presentación personal
b) Exposición: el problema a resolver, hipótesis, objetivos, resultados, conclusiones, los aportes, contribución a la ciencia y/o solución a un problema social y Recomendaciones
c) Grado de convicción y sustento bibliográfico utilizados para las respuestas a las interrogantes del Jurado y público asistente
d) Dicción y dominio de escenario

Así mismo, el Jurado plantea a la tesis o trabajo de investigación las observaciones siguientes:

.....

.....

.....

Obteniendo en consecuencia el Maestrista la Nota de **15 (quince)**
Equivalente a **aprobado**

(aprobado ó desaprobado)

Los miembros del Jurado, firman el presente **ACTA** en señal de conformidad, en Pucallpa, siendo las 12:00 m. horas del 12 de marzo del 2021

PRESIDENTE

SECRETARIO

VOCAL

UNIVERSIDAD NACIONAL DE UCAYALI
VICERRECTORADO DE INVESTIGACION
DIRECCION GENERAL DE PRODUCCION INTELECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACION

SISTEMA ANTIPLAGIO URKUND

N°0119-2020

La **Dirección General de Producción Intelectual**, hace constar por la presente, que el Informe Final (Tesis), titulado:

LOS SISTEMAS DE CIFRADO ROCE EN LA SEGURIDAD DE ARCHIVOS DE TEXTO.

Cuyo autor (es)	:	TOMINAGA GARCIA, YUMI
ESCUELA	:	POSGRADO
MAESTRIA	:	INGENIERIA DE SISTEMAS
MENCION	:	CIENCIAS DE LA COMPUTACIÓN
ASESOR	:	Dr. Ayra Apac, Nilton Cesar

Después de realizado el análisis correspondiente en el Sistema Antiplagio URKUND, dicho documento presenta un **porcentaje de similitud de 08%.**

En tal sentido, de acuerdo a los criterios de porcentaje establecidos en el artículo 9 de la DIRECTIVA DE USO DEL SISTEMA ANTIPLAGIO URKUND, el cual indica que no se debe superar el 10%. Se declara, que el trabajo de investigación: SI Contiene un porcentaje aceptable de similitud, por lo que SI se aprueba su originalidad.

En señal de conformidad y verificación se FIRMA Y SELLA la presente constancia.

Fecha: 11/03/2020

UNIVERSIDAD NACIONAL DE UCAYALI
DIRECCION GENERAL DE PRODUCCION INTELECTUAL
DRA. DINA PAEZ QUISPE
Dirc. Gral. Prod. Intel

AUTORIZACIÓN DE PUBLICACION DE TESIS

REPOSITORIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI

Yo, Yumi Tominaga García

Autor(a) de la TESIS de maestría titulada:

"Los sistemas de cifrado RSCE en la seguridad de archivos de texto"

Sustentada el año: 2021

Con la asesoría de: DR. Nilton Cesar Ayra Apac

En la Escuela de Posgrado, Maestría: Ciencias de la Computación

Mención: Maestro en Ciencia de la computación

Autorizo la publicación:

PARCIAL ☐ Significa que se publicará en el repositorio institucional solo La caratula, la dedicatoria y el resumen de la tesis. Esta opción solo es válida **marcar si su tesis o documento presenta material patentable**, para ello deberá presentar el trámite de CATI y/o INDECOPI cuando se lo solicite la DGPI UNU.

TOTAL ☒ Significa que todo el contenido de la tesis y/o documento será publicada en el repositorio institucional.

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali **licencia no exclusiva** para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempo y las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la **tesis es una creación de mi autoría** y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali y del Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 11 / 07 / 2022

Email: ytominagag@gmail.com Firma:

Teléfono: 961659126 DNI: 41792179

AGRADECIMIENTO

Agradecer a Dios por bendecirme con salud y poder disfrutar de la vida cada día junto a mis seres queridos, a mi querido papá que desde el cielo me guía y protege mis pasos, a mi querida mamá que me alienta a mejorar día a día, a mis hermanos que me aconsejan a seguir adelante, a mi esposa e hijos que son el motor y motivo para poder crecer y superarme personal, académica y profesionalmente.

RESUMEN

En estos tiempos, donde la información es el bien que tiene el más alto valor en una compañía, se requiere protegerlo, con el avance de las telecomunicaciones las transacciones de información se hacen cada vez más rápido y en mayor cantidad, por lo que se requiere protegerlo.

Nuestra investigación se basa en la aplicación de uno de los algoritmos de encriptación de archivos de texto más usados que es el Cifrado ROCE.

Muchos usuarios dejan que el sistema operativo, navegador o el sistema de correos administre la seguridad de las transacciones de información, muchas veces no está bien configurado para tal fin, volviéndose vulnerable el envió o recepción de información.

Toda la investigación lo desarrollamos en el laboratorio WiFi de la Facultad de Ingeniería de Sistemas e Ingeniería Civil, aplicándolo en las transacciones de información tipo texto que desarrollaron los usuarios.

La investigación fue de tipo explicativa, con un estudio de campo, analizando en toda la investigación la influencia de los sistemas de cifrado ROCE en la la seguridad de los archivos de texto.

Entre los resultado alcanzados podemos manifestar que El software de encriptación más usado es Gpg4Win, con un 26.2% (100 veces usado), siguiendo ENIGMA con 17.8 % (68 veces) y Steganos Safe con 17.6% (67 veces), podemos afirmar que el uso de Gpg4win se da como primer lugar por ser el más usado por la mayoría de empresas dedicados a cyberseguridad, mientras que ENIGAMA, lo hacen por un entorno más comercial; Del total de algoritmos analizados, el algoritmo más usado en este estudio fue el ROCE con

un 19.2 % (73 veces), PGP con un 18.1% (69 veces) y 17.3% (66 veces) tanto PSK y AES; Por lo que podemos afirmar que al hacer uso de un algoritmo de encriptación para dar seguridad de datos tipo texto, se usa el ROCE en un alto porcentaje, así mismo ninguno de los usuarios del laboratorio wifi, nos informó que tuvieron problemas en el envió o recepción de información.

PALABRAS CLAVES: Seguridad de Archivos, Encriptación.

ABSTRACT

In these times, where information is the good that has the highest value in a company, it is necessary to protect it, with the advance of telecommunications, information transactions are becoming faster and in greater quantity, which is why it is required protect it.

Our research is based on the application of one of the most used encryption algorithms for text files, which is the ROCE encryption.

Many users let the operating system, browser or the mail system manage the security of information transactions, often not well configured for that purpose, making the sending or receiving of information vulnerable.

We carried out all the research in the WiFi lab of the Faculty of Systems Engineering and Civil Engineering, applying it to the text-type information transactions that the users developed.

The investigation was of explanatory type, with a field study, analyzing in all the investigation the influence of the systems of encryption ROCE in the security of the text files.

Among the results achieved we can state that the most used encryption software is Gpg4Win, with 26.2% (100 times used), following ENIGMA with 17.8% (68 times) and Steganos Safe with 17.6% (67 times), we can affirm that the use of Gpg4win is given as the first place because it is the most used by most companies dedicated to cybersecurity, while ENIGAMA, they do it for a more commercial environment; Of the total algorithms analyzed, the algorithm most used in this study was the ROCE with 19.2% (73 times), PGP with 18.1% (69 times) and 17.3% (66 times) both PSK and AES; So we can say that by using an encryption

algorithm to give text type data security, the ROCE is used in a high percentage, likewise none of the users of the wifi lab informed us that they had problems in sending or Reception of information.

KEYWORDS: File Security, Encryption.

INTRODUCCION

La presente investigación se centró en evaluar los sistemas de seguridad de archivos de texto en las transacciones de información que desarrollaron los usuarios en el laboratorio WiFi de la Facultad de Ingeniería de Sistemas y de Ingeniería Civil de la Universidad Nacional de Ucayali.

En nuestro caso se planteó la aplicación de los sistemas de encriptación de texto usando el algoritmo ROCE.

La investigación se inicia con el: Capítulo I, Problema de Investigación, se detalla la necesidad de priorización del problema con sus respectivas interrogantes, formulación del problema, justificación del estudio, limitaciones, antecedentes y objetivos. Capítulo II, Marco Teórico, detalla los antecedentes históricos. Capítulo III, Marco Metodológico, precisa las variables, la metodología de estudio concerniente a la investigación acción participativa y al diseño retrospectivo - descriptivo, población y muestra, método de estudio, técnicas e instrumentos respecto a los anexos, ficha de observación, encuestas, entrevistas para la recolección de datos y métodos de análisis de datos. Capítulo IV, Resultados, Capítulo V Discusión de resultados, conclusiones y sugerencias, y al final los Anexos.

INDICE

AGRADECIMIENTO ii
RESUMEN iii
ABSTRACT v
INTRODUCCION vii
INDICE viii
INDICE DE TABLAS x
INDICE DE GRÁFICOS xi
CAPÍTULO I 1
EL PROBLEMA DE INVESTIGACIÓN 1
1.1. DESCRIPCIÓN DEL PROBLEMA. 1
1.2. FORMULACIÓN DEL PROBLEMA. 2
- **Problema General** 2
- **Problemas Específicos** 2

1.3. OBJETIVOS 2
- **Objetivo General.** 2
- **Objetivos Específicos.** 2

1.4. HIPÓTESIS Y/O SISTEMA DE HIPÓTESIS. 3
- ✓ **Hipótesis general** 3
- ✓ **Hipótesis Nula:** 3
- ✓ **Hipótesis Secundaria:** 3

1.5. VARIABLES. 3
- ✓ **Variable Independiente** 3
- ✓ **Variable dependiente** 5
- ✓ **Variable interviniente** 7

1.6. OPERACIONALIZACION DE VARIABLES 8
1.7. JUSTIFICACIÓN E IMPORTANCIA. 8
1.8. VIABILIDAD. 9
1.9. LIMITACIONES 10
MARCO TEÓRICO 11
2.1. ANTECEDENTES 11
2.2. BASES TEÓRICAS. 23
2.3. BASES EPISTÉMOLOGICAS 27
CAPÍTULO III 33
MARCO METODOLÓGICO 33
3.1. TIPO DE INVESTIGACIÓN 33
3.2. DISEÑO DE LA INVESTIGACIÓN 33

3.3. POBLACIÓN Y MUESTRA **34**
✓ **POBLACION** **34**
✓ **MUESTRA** **35**
3.4. INSTRUMENTOS DE RECOLECCIÓN DE DATOS **36**
VALIDACION Y CONFIABILIDAD DEL INSTRUMENTO ESTADISTICO **37**
3.5. TÉCNICAS DE RECOJO, PROCESAMIENTO Y PRESENTACIÓN DE DATOS. **38**
CAPÍTULO IV **39**
RESULTADOS **39**
4.1. RECOLECCIÓN, PRESENTACIÓN Y TRATAMIENTO DE DATOS 39
4.2. PRESENTACIÓN DE RESULTADOS 39
INTERPRETACION PARCIAL **42**
4.3. VERIFICACION DE LA HIPOTESIS 44
CAPÍTULO V **47**
DISCUSIÓN DE RESULTADOS. **47**
CONCLUSIONES. 49
BIBLIOGRÁFIA **51**
ANEXOS **53**
ANEXO: 01 – MATRIZ DE CONSISTENCIA **54**
ANEXO: 02 - FICHA TECNICA DATO DE ARCHIVOS **55**
ANEXO: 03 - VALIDACION DEL INSTRUMENTO POR JUICIO DE EXPERTOS **56**

INDICE DE TABLAS

TABLA 1. OPERACIONALIZACIÓN DE VARIABLES (INDICADORES) 8

TABLA 2. ARCHIVOS CON CIFRADO ROCE ENVIADO/RECIBIDO 35

TABLA 3. METODO DE ENCRIPTACION SEGÚN SOFTWARE UTILIZADO 40

TABLA 4. METODO DE ENCRIPTADO USADO 42

TABLA 5. USO DEL ROCE POR VS SOFTWARE DE ENCRIPTACION 44

INDICE DE GRÁFICOS

GRÁFICO 1. METODO DE ENCRIPTACION SEGÚN SOFTWARE UTILIZADO 41

GRÁFICO 2. METODO DE ENCRIPTADO USADO 43

GRÁFICO 3. USO DEL ROCE VS SOFTWARE DE ENCRIPTACION 45

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. DESCRIPCIÓN DEL PROBLEMA.

Con la masificación de los sistemas inalámbricos, los sistemas de encriptación se han vuelto una necesidad vital para su funcionamiento, ya se para el acceso a la red o para el envío y recepción de información.

Los sistemas de encriptación tienen sus fundamentos en las matemáticas, para ser planteados bajo algoritmos complejos, recursivos, genéticos, etc.

En nuestro caso se plantea la aplicación de los sistemas de encriptación de texto usando el algoritmo ROCE.

La importancia de la presente investigación se da por los procesos de seguridad del manejo de información se dan debido a que se exige en la actualidad mayor seguridad en la transacción de información, no solamente se necesita que se sepa el código de acceso a la red sino conocer además la llave que abrirá el archivo y aplicara un algoritmo para encriptar o desencriptarlo.

Las transacciones de información se dan en cada momento, usando todos los medios de comunicación, la valorización de la información dependerá de cada usuario, por lo que podrá aplicar una serie de técnicas de seguridad, unas más complejas que otras, siendo la de mayor complejidad la que consume mayor costo computacional por la magnitud de sus algoritmos.

El uso de cifrado de datos, por lo regular se da por defecto y en forma gratuita en la mayoría de los APP y en los servidores de correo electrónico, por lo que podríamos decir que la frecuencia de uso de seguridad es permanente, variando los algoritmos usados, unos más que otros.

1.2. FORMULACIÓN DEL PROBLEMA.

- **Problema General**

  ¿En qué medida el uso del cifrado ROCE, ayuda en la seguridad de archivos de texto?

- **Problemas Específicos**
  - ¿Cuál es el grado de asociación entre el uso de cifrado Roce y la Seguridad Tipo Texto?
  - ¿Cuáles Son los resultados del uso de los sistemas de cifrado Roce en la seguridad de archivos de texto?

1.3. OBJETIVOS

- **Objetivo General.**

  Determinar la influencia de los sistemas de cifrado ROCE en la seguridad de los archivos de texto.

- **Objetivos Específicos.**
  - Identificar el grado de asociación entre el uso cifrado Roce y la seguridad de archivos tipo texto.
  - Conocer los resultados del uso de los sistemas de cifrado Roce en la seguridad de archivos de texto.

1.4. HIPÓTESIS Y/O SISTEMA DE HIPÓTESIS.

- ✓ **Hipótesis general**

  La aplicación de los sistemas de encriptación Roce influye significativamente en la seguridad de archivos de texto.

- ✓ **Hipótesis Nula:**

  La Aplicación de los sistemas de encriptación ROCE no influye significativamente en la seguridad de archivos de texto.

- ✓ **Hipótesis Secundaria:**

  - ➢ El grado de asociación entre el uso cifrado Roce y la seguridad de archivos tipo texto es alta.
  - ➢ El uso de los sistemas de cifrado Roce en la seguridad de archivos de texto tiene un alto porcentaje de uso.

1.5. VARIABLES.

- ✓ **Variable Independiente**

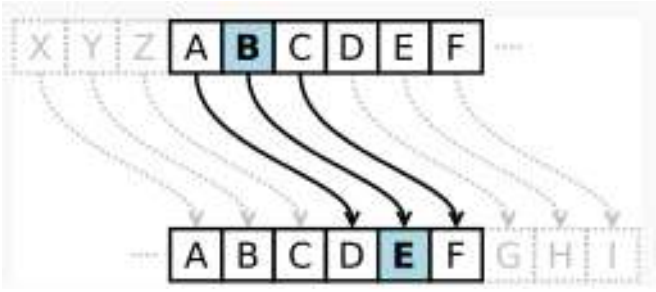
  Sistemas de cifrado ROCE

  Definición:

  En criptografía, el cifrado César, también conocido como cifrado por desplazamiento, código de César o desplazamiento de César, es una de las técnicas de cifrado más simples y más usadas. Es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Por ejemplo, con un desplazamiento de 3, la A sería sustituida por la D (situada 3

lugares a la derecha de la A), la B sería reemplazada por la E, etc. Este método debe su nombre a Julio César, que lo usaba para comunicarse con sus generales.

Figura 1: Cifrado César



Fuente:http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/cesar.html

El cifrado César muchas veces puede formar parte de sistemas más complejos de codificación, como el cifrado Vigenére, e incluso tiene aplicación en el sistema ROT13. Como todos los cifrados de sustitución alfabética simple, el cifrado César se descifra con facilidad y en la práctica no ofrece mucha seguridad en la comunicación.

La codificación también se puede representar usando aritmética modular, transformando las letras en números, de acuerdo al esquema A = 0, B = 1,..., Z = 26.1 La codificación de la letra x con un desplazamiento n puede ser descrita matemáticamente como:

$$E_n(x) = x + n \mod 27.$$

La decodificación se hace de manera similar:

$$D_n(x) = x - n \mod 27.$$

La operación de sustitución se conserva siempre a lo largo de todo el mensaje, por lo que el cifrado se clasifica como un cifrado de tipo sustitución monoalfabética, en oposición a la sustitución polialfabética.

(http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/cesar.html)

- ✓ **Variable dependiente**

Seguridad de archivos de texto.

Definición Conceptual:

Es un archivo informático que contiene únicamente texto formado solo por caracteres que son legibles por humanos, careciendo de cualquier tipo de formato tipográfico.1 El término texto llano proviene de una traducción literal del término inglés “plain text”, término que en lengua castellana significa texto simple o texto sencillo.

Estos archivos están compuestos de bytes que representan caracteres ordinarios como letras, números y signos de puntuación (incluyendo espacios en blanco), también incluye algunos caracteres de control como tabulaciones, saltos de línea y retornos de carro. Estos caracteres se pueden codificar de distintos modos dependiendo de la lengua usada. Los sistemas de codificación más usados son: ASCII, ISO-8859-1 o latín-1 y UTF-8.

Los archivos de texto plano carecen de información destinada a generar formatos (negritas, subrayado, cursivas, tamaño, etc.) y tipos de letra (por ejemplo, Arial, Times, Courier, etc.). Esta simplicidad permite que una gran variedad de programas pueda leer y editar ese contenido. Las aplicaciones destinadas a la escritura y modificación de archivos de texto se llaman editores de texto.

Adicionalmente, cuando ocurre algún tipo de corrupción de datos, es más fácil para una persona arreglar problemas en un archivo de texto que en uno binario. Algunos formatos de texto (como XML) tienen mecanismos incluidos para especificar la codificación del documento, pero la gran mayoría de formatos no lo tiene. Como contrapartida, cualquier usuario podría leer y modificar el valor de las variables a su antojo, o aleatoriamente o por equivocación, siendo impredecibles los efectos sobre el programa.

Un inconveniente de los archivos de texto es que no hay forma segura de saber a priori que codificación se utilizó para guardarlo. Un programa editor de texto puede grabar un archivo en UTF-8, pero un compilador puede esperar un formato ISO-8859; al tratar de compilar el archivo generará errores en el programa. El problema es aún más complejo en el caso de ficheros transmitidos a través de redes informáticas, en las que una identificación

errónea de la codificación de los archivos de texto puede dar lugar a multitud de errores.

- ✓ **Variable interviniente**

  Universidad Nacional de Ucayali.

  Definición Conceptual:

  La Universidad Nacional de Ucayali es una de las principales universidades del Perú, ubicada en el departamento de Ucayali. Fue creada por el decreto Ley Nº 22804 el 18 de diciembre de 1979, bajo el nombre de Universidad Nacional de Pucallpa durante el gobierno militar del General Francisco Morales Bermúdez.

  Mediante Ley N° 223261 del 17 de julio de 1981, durante el gobierno democrático del Arquitecto Fernando Belaunde Terry, el Congreso de la República eleva al rango de Ley la norma de creación de la Universidad Nacional de Pucallpa.

  Según la Ley N° 23733 Ley Universitaria del 09 de diciembre de 1983, cambia de denominación a la Universidad Nacional de Pucallpa por Universidad Nacional de Ucayali, denominación que hasta la fecha persiste. Mediante Resolución N° 292-93 del 26 febrero de 1993, la Asamblea Nacional de Rectores autoriza el funcionamiento definitivo de la Universidad Nacional de Ucayali.

Actualmente la Universidad Nacional de Ucayali cuenta con ocho Facultades, Una Escuela de Posgrado y Ocho Unidades de Investigación.

1.6. OPERACIONALIZACION DE VARIABLES

TABLA 1. OPERACIONALIZACIÓN DE VARIABLES (INDICADORES)

Variable	Dimensiones	Indicadores
Sistema de encriptación ROCE	Algoritmo	• Eficiencia • Efectividad
Seguridad de Archivos de Texto	Protección	• Nivel de seguridad • Portabilidad

1.7. JUSTIFICACIÓN E IMPORTANCIA.

En la actualidad se usan algoritmos de encriptación simétrica, utilizando los procesos de intercambio para el proceso de encriptación de la información, en esta investigación se pretende proponer la aplicación de un proceso de cifrado para archivos de texto con un algoritmo ligero que no requiere computación pesada para poder encriptar o desencriptar.

Así mismo, el estándar internacional AES, utiliza un cifrado con un nivel aceptable de seguridad, porque protege la encriptación frente a ataques conocidos a la fecha, pero que requiere alto consumo de procesamiento para su protección.

Frente a un ataque de fuerza bruta (probando una clave a la vez) la seguridad AES exige 2128 intentos por cada código, esto es poco si

pensamos que los atacantes usan un robot en software para el ataque. En nuestro caso aplicaremos un cifrado de clave pública para iniciar el proceso de encriptación y/o desencriptación de texto.

1.8. VIABILIDAD.

Es viable porque va permitir estudiar el análisis, diseño e implementación del cifrado ROCE y su impacto en la seguridad de archivos de texto.

- ✓ **Científica**

  Se ha tenido a disposición los conocimientos científicos y bibliografía actualizada e investigaciones pertinentes al caso de estudio, con carácter y articulación: interdisciplinaria, multidisciplinaria y transdisciplinaria en armonía con la investigación.

- ✓ **Técnica**

  Se ha contado con las técnicas, instrumentos, herramientas, métodos, procedimientos, metodología y asesoramiento profesional, para enfocar al proceso de investigación sobre las variables en estudio que permitió describir el tema dando sentido y comprensión al conocimiento que se arribe con los resultados para su interpretación y entendimiento.

- ✓ **Económica**

  Se ha dispuesto de los recursos materiales y económicos necesarios, que permitió sufragar los egresos y asumir los esfuerzos que demandó el desarrollo de la presente investigación.

- ✓ **Social**

  Porque ha respondido a la demanda de la nuestra sociedad y en consecuencia es necesidad de la población.

- ✓ **Personal**

  Se ha tenido las competencias, capacidades y experiencia investigador por ser egresado de la maestría en Ciencia de la Computación y por la experiencia laboral en el manejo colaborativo de proyectos de ingeniería de software.

- ✓ **Procedimental**

  Existen los procedimientos operacionales para el proceso de investigación, el cual se ha desarrollado conforme al esquema establecido en el Reglamento de Elaboración de Tesis para Maestristas, lo que genera validez interna y externa de la investigación.

1.9. LIMITACIONES

Las más importantes limitaciones de esta investigación son las siguientes:

- ✓ Escasez de antecedentes de la investigación (revistas especializadas, tesis, internet).
- ✓ Escasez de material bibliográfico y científico. Específicamente sobre conceptos, categorías, etc.
- ✓ Inexistencia de pruebas estandarizadas y validadas para medir las capacidades de la aplicación.

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES

ANTECEDENTES NACIONALES

- Inoguchi A. (2017) GESTIÓN DE LA CIBERSEGURIDAD Y PREVENCIÓN DE LOS ATAQUES CIBERNÉTICOS EN LAS PYMES DEL PERÚ, 2016, UNIVERSIDAD SAN IGNACIO DE LOYOLA, El presente trabajo de investigación ayudará a las PYMES del Perú a tomar conciencia en la protección de su data informática y sistemas informáticos, teniendo en cuenta que cuando nos referimos a la data informática, es toda la información virtual que se encuentra almacenada y disponible en la red privada de las pymes, siendo dicha información fundamental y vital para que las pymes funcionen correctamente y alcance sus objetivos propuestos.

  El objetivo es de obtener un nivel considerable de seguridad para las pymes, el cual se logrará con los resultados obtenidos en la investigación y posteriormente recomendando e indicando una propuesta para gestión y prevención de seguridad informática, la cual podrá ser aplicable para la mayoría de pymes de diferentes rubros o giros de negocio, el único requisito es que la pyme se proponga implementar la propuesta de seguridad informática resultante.

En el primer capítulo se explicará la problemática, la cual nos habla de los motivos de una fácil intromisión a la información en una red privada, la importancia de plasmar criterios de seguridad de la información para mantener una red privada segura. Así como también teóricamente el objetivo, los antecedentes e hipótesis de esta investigación. En el segundo capítulo se desarrollará la metodología con la que se ha llevado a cabo la investigación como la operacionalización de las variables y técnicas de recolección de datos hasta los métodos que emplearemos para el análisis del mismo. En el tercer capítulo se da a conocer y explicar los resultados de esta investigación, posterior a ello se procederá de igual forma a explicar las conclusiones y por último se brindara todas las recomendaciones posibles de la práctica realizada en fin de tener pymes en el Perú con una alto conocimiento de protección de su información en las redes de internet privadas y así evitando la intromisión y robo de su data virtual por parte de extraños a la pyme.

- Vega, L.; Zavaleta, F. (2012) UNIVERSIDAD NACIONAL DE TRUJILLO, Diseño de prototipo de un sistema de detección de intrusos distribuido para la seguridad de redes móviles AD-HOC, En el presente trabajo diseñamos un sistema de detección de intrusos distribuido para redes móviles Ad-Hoc, el cual usa algoritmos basados en la capacidad de los nodos y emplea técnicas de detección para determinados modelos de ataques.

La seguridad en redes Ad-Hoc, específicamente en el desarrollo de IDSs, es actualmente uno de los temas más importantes de investigación debido a la gran variedad de aplicaciones que tiene en los campos militar, industrial, etc.

El diseño aborda los criterios para definir el ámbito de detección de los nodos IDS, recolección y análisis de datos, selección de nodos IDS, diseño de sensor y técnicas de detección de intrusos. Para la selección de nodos se emplea un algoritmo heurístico que permite identificar un subconjunto de nodos que ejecutarán el IDS tal que cubran la totalidad de la red; en el caso de las técnicas de detección usaremos las de uso indebido las cuales permiten identificar ataques de manera precisa tales como “Packet Dropping” y “ARP Spoofing”.

Para poder evaluar el funcionamiento correcto de nuestro sistema de detección de intrusos se desarrolló un simulador en el cual plasmamos cada algoritmo listado en éste documento. Este simulador permite ver el proceso de selección de los nodos IDS dentro de la red Ad-hoc, así como la detección de ataques basados en firmas.

La conclusión a las cual hemos llegado luego de haber realizados las pruebas y el análisis de los resultados es que el diseño propuesto si ha permitido mejorar la seguridad de las redes MANET al tener un grado positivo de efectividad en la detección de intrusos.

- León K. (2005), PONTIFICIA UNIVERSIDAD CATOLICA DEL PERU, ESCUELA DE GRADUADOS, ENCRIPTACION RSA, DE ARCHIVOS DE TEXTO, Este trabajo de tesis fue iniciado en agosto del 2004, en base a un programa en lenguaje C elaborado en el curso Seminario de Tesis. Desde ese programa en C hasta la versión actual en lenguaje java, han habido muchos cambios, mejoras, revisiones y correcciones que hacen que el sistema que ahora se presenta sea un programa completamente nuevo.

  Los algoritmos de encriptación tienen una base fuertemente matemática y de esto no escapa el RSA, poder manejar estos conceptos dentro de este programa no ha sido precisamente de las tareas más sencillas, sino por el contrario demandó mucho tiempo no solo en entender el funcionamiento del algoritmo sino también en la implementación y pruebas del mismo.

  Siendo el algoritmo implementado una técnica de encriptación muy elaborada, empezaremos esta introducción comentando muy brevemente sobre el nacimiento de la criptografía. Los códigos secretos han sido utilizados desde la antigüedad para enviar mensajes seguros, por ejemplo en tiempo de guerra o de tensiones diplomáticas. Hoy día se guarda, con frecuencia, información delicada de naturaleza médica o financiera en los ordenadores, y es importante mantenerla en secreto.

  Muchos códigos están basados en teoría de números. Uno muy simple es sustituir cada letra del alfabeto por la siguiente o por tres letras después. Estos códigos son fáciles de romper pues se

pueden probar todos los posibles valores hasta obtener un mensaje comprensible, o podemos comparar las letras más frecuentes en el mensaje con las que se saben que son más frecuentes en la lengua original.

Históricamente primero han aparecido los códigos basados en una única clave conocidos como sistemas de clave privada. Estos tienen el inconveniente de que el remitente y el receptor deben estar de acuerdo, con anterioridad, en los valores de la clave. Teniendo en cuenta que por seguridad deberán cambiar la clave de vez en cuando, ¿de qué modo podrían hacerlo de una manera segura?

Esta dificultad se supera con la aparición de los sistemas criptográficos de clave pública que permite a todos los remitentes utilizar la clave pública del emisor para la encriptación de un mensaje que sólo el destinatario podrá recuperar pues será el único poseedor de la clave privada.

ANTECEDENTES INTERNACIONALES

- Macen C. (2014) UNIVERSIDAD INTERCONTINENTAL – PARAGUAY, POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, La información es un activo que, como otros activos de la institución, es esencial que sea protegido adecuadamente. Esta investigación nace de la necesidad de elaborar políticas de seguridad de la información para el Departamento de Tecnología Informática de la UTIC. Por ello se propone describir la realidad que presenta la UTIC para la construcción de política de seguridad de la información. Se

contempló como núcleo investigativo los funcionarios de la Sedes de la Regional Central, la población quedó compuesta de 84 (ochenta y cuatro) funcionarios que manejan sistemas de informaciones y 10 (diez) funcionarios del Departamento de Tecnología Informática. Esta investigación es con un enfoque cuantitativo, de nivel descriptivo, el diseño es no experimental. El resultado demostró una proporción global con respecto al manejo de la información de manera insegura 55,95 % y una proporción del manejo seguro de 44,05 %. Como recomendación se presenta el manual de políticas de seguridad de la información para su implementación.

- Álvarez L. (2005) UNIVERSIDAD IBEROAMERICANA, SEGURIDAD EN INFORMÁTICA, La auditoría informática tiene como principal objetivo, evaluar el grado de efectividad de las tecnologías de información, dado que evalúa en toda su dimensión, en qué medida se garantiza la información a la organización, su grado de eficacia, eficiencia, confiabilidad e integridad para la toma de decisiones, convirtiéndola en el método más eficaz para tales propósitos.

  Su ámbito de acción se centra, en revisar y evaluar: los procesos de planificación; inversión en tecnología; organización; los controles generales y de aplicación en proyectos de automatización de procesos críticos; el soporte de las aplicaciones; aprovechamiento de las tecnologías; sus controles específicos, los riesgos inherentes

a la tecnología, como la seguridad de sus recursos, redes, aplicaciones, comunicaciones, instalaciones y otras.

La generalizada informatización de los procesos y disciplinas que impactan directamente en la sociedad, en especial las relacionadas con la gestión económica, que hace apenas una década se procesaban manualmente, así como los propios cambios que introduce su tratamiento informatizado, introducen transformaciones sustanciales sobre el concepto tradicional del control interno, la estructura del registro y consecuentemente la práctica de las auditorias.

La auditoría interna, en su desempeño, tiene también la responsabilidad de velar por el adecuado empleo y utilización de los recursos informáticos y por el cumplimiento de la misión que a éstos le ha asignado la organización.

Tal conclusión conduce, a la inexcusable necesidad de practicar “auditorias informáticas”, a partir de un conjunto de técnicas y procedimientos que evalúen los controles internos intrínsecos y específicos de los sistemas de información; en consecuencia, determina, que conceptualmente, no es dependiente ni evoluciona desde la auditoria convencional; sus puntos de partida son esencialmente diferentes ya que no analiza la corrección o incorrección de cuentas contables, sino que constituye un instrumento de control superior para valorar la correcta administración de los recursos de tecnología de información como: Datos, aplicaciones, tecnología, instalaciones, y personal para

valorar la efectividad de la información que requiere la organización. Su concepción se refiere a la integración de las técnicas informáticas y de auditoria para practicar un nuevo estilo de verificación, sobre un ambiente no convencional, con herramientas de punta y con procedimientos inexistentes y que puede definirse como: “El conjunto de procedimientos y técnicas que evalúan, parcial o totalmente los controles internos de los sistemas de información; la protección de sus activos y recursos; verifica si su explotación se desarrolla con eficiencia, de acuerdo con las políticas y normativas establecidas por cada entidad y valora si se alcanza el grado de organización previsto para el marco donde participa y actúa”.

En correspondencia con la definición que antecede, así como por su finalidad, objetivos y utilidad que le atribuimos, la auditoria informática se clasifica en: auditorias informáticas de seguridad, de redes, de sistemas o aplicaciones, de explotación de los sistemas, de planificación y organización y de gestión de la tecnología para el logro de los propósitos de la organización. Consecuentemente, se han diseñado un conjunto de premisas, principios, y procedimientos para la práctica de estas auditorías.

En cuanto a la seguridad en informática, las computadoras y la Internet son ahora una parte familiar de nuestras vidas. Quizá no las veamos a menudo, pero ahí están; involucradas de alguna manera en la mayoría de nuestras actividades diarias, en los negocios de cualquier empresa, en las instituciones educativas, en las diferentes

áreas de gobierno, sin el apoyo de éstas herramientas ninguna de ellas sería capaz de manejar la impresionante cantidad de información que parece caracterizar a nuestra sociedad. Pero también existe una problemática en ellas, la seguridad; para ello se han desarrollado firewalls dispositivos de software que protegen la integridad de las mismas. Cada vez más personas necesitaran conocer el manejo de las computadoras así como las protecciones que día a día se van ofreciendo para garantizarnos la seguridad en el manejo de la información.

Los inconvenientes en cuestión de seguridad no son conocidos por todos los usuarios de la red y por ello no saben cómo protegerse de dicha vulnerabilidad que tienen cada vez que se conectan a esta red de trabajo.

Convendría hablar un poco de qué se entiende por Seguridad. En esta investigación se entenderá por seguridad en redes, a la protección frente ataques e intrusiones en recursos corporativos por parte de intrusos a los que no se permite acceso a dichos recursos. La seguridad siempre será relativa al tipo de servicios que queremos ofrecer a los usuarios autorizados, según se establece en la política de seguridad de la empresa.

Creo conveniente definir primeramente las partes elementales que se relacionan con la seguridad en informática. En primer lugar tenemos la WAN (World Area Network) es una gran red de cómputo de cobertura mundial y una de las más comunes es Internet. En segundo lugar, está LAN (Local Area Network) qué es una red

mediana denominada local ya que está limitada a una pequeña área geográfica y normalmente es utilizada por empresas privadas, públicas, educativas, etc. Estas dos redes llegan a interactuar utilizando un conjunto de protocolos de comunicación de datos.

TCP/IP es de los protocolos más comunes. Sus siglas significan Protocolo de Control de Transmisión y Protocolo de Internet (Transmisión Control Protocol / Internet Protocol). Estos protocolos permiten el enrutamiento de información de una máquina a otra, la entrega de correo electrónico y noticias, e incluso la conexión remota.

La idea de este trabajo es que toda persona que se interese en este tema aprenda en forma rápida, simple y a valorar lo importante que es la información, tanto para las grandes como pequeñas y medianas empresas y contar con sistemas de seguridad que alejen visitas de posibles hackers.

- Moreno M. (2010) UNIVERSIDAD DE CHILE, DISEÑO E IMPLEMENTACION DE UN ESQUEMA DE ENCRIPTACION Y FIRMAS BASADO EN IDENTIDAD ARA DISPOSITIVOS BUG. Históricamente, la autentificación de mensajes se ha manejado a través de firmas digitales basadas en certificados, usualmente emitidos por una entidad neutral a la comunicación y de confianza de todas las partes. Sin embargo, esta solución no siempre es posible de implementar, debido a factores como los costos, el tiempo limitado de vigencia de los certificados, la necesidad de

depositar la confianza en un tercero, y por último el poder, usualmente limitado, de procesamiento de las máquinas. Además los certificados usualmente son muy pesados, y deben adjuntarse a cada mensaje enviado para mostrar su autenticidad, lo cual dificulta su implementación en dispositivos con poca capacidad de almacenamiento.

La Criptografía basada en identidad (o Identity Based Cryptography, IBC) es una alternativa al escenario presentado en sistemas que desean autentificar mensajes, pero no quieren (o no pueden) depender de certificados. Esto se logra usando la identidad de la persona (o del dispositivo) como semilla para la generación de claves por parte de un servidor maestro dentro del mismo sistema. De esta forma, las firmas son mucho más ligeras que los certificados, agilizando las comunicaciones. Además, como las identidades son públicas, cualquier miembro de la red puede verificar la autenticidad de un mensaje sin necesidad de hacer consultas online al ente central.

Por otro lado, las lecturas biométricas son la forma más usada de comprobar la identidad de una persona, ya sea a través de las huellas digitales, reconocimiento facial, lectura de iris o incluso análisis de forma de las orejas. Esto debido a que los rasgos mencionados son únicos para la persona, e incluso los dispositivos actuales permiten reconocer rasgos latentes, es decir que no poseen señales biológicas, de "vivos" y así prevenir el uso de guantes, máscaras, etc.

El tema de esta tesis es desarrollar una alternativa de sistema de seguridad para dispositivos de procesamiento limitado. El sistema utiliza firma de mensajes basada en identidad, pero usando las huellas digitales tanto para enlazar un usuario específico a un dispositivo, como para la protección de los datos privados del usuario. El sistema debe poder extenderse para poder incorporar encriptación basada en identidad también.

La primera parte de este trabajo consiste en un estudio de las componentes a usar, tanto de hardware como de software, incluyendo los conceptos básicos necesarios para su diseño y operación, así como los estándares que siguen. La segunda parte corresponde a un estudio y descripción detallada de las componentes del proyecto y de la implementación realizada, para terminar con posibles extensiones.

El sistema se probará en dispositivos BUG, un tipo de hardware usado en el diseño y fabricación de prototipos modulares.

- Soto J. (2010), INSTITUTO POLITECNICO NACIONAL DE MEXICO, ALGORITMO DE ENCRIPTACION SIMÉTRICO QE PROCESA BLOQUES DE 192 BITS, CON LLAVES DE CIFRADO DE 192 BITS, EMPLEANDO LOS TEOREMAS FACTORIAL Y JV.

  El presente trabajo documenta el diseño de un algoritmo de encriptación simétrico que procesa bloques de 182 bits, con llaves de cifrado de 192 bits, empleando los teoremas factorial y JV.

2.2. BASES TEÓRICAS.

- **CIFRADO.**

  En criptografía, el cifrado es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) transforma un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo. Las claves de cifrado y de descifrado pueden ser iguales (criptografía simétrica), (criptografía asimétrica) o (Criptografía híbrida).

  El juego de caracteres (alfabeto) usado en el mensaje sin cifrar puede no ser el mismo que el juego de caracteres que se usa en el mensaje cifrado.

  A veces el texto cifrado se escribe en bloques de igual longitud. A estos bloques se les denomina grupos. Estos grupos proporcionaban una forma de verificación adicional, ya que el texto cifrado obtenido debía tener un número entero de grupos. Si al cifrar el texto plano no se tiene ese número entero de grupos, entonces se suele rellenar al final con ceros o con caracteres sin sentido.

  Aunque el cifrado pueda volver secreto el contenido de un documento, es necesario complementarlo con otras técnicas criptográficas para poder comunicarse de manera segura. Puede

ser necesario garantizar la integridad la autenticación de las partes, etc.

Tipos de cifrado según sus claves:

Un sistema de cifrado se denomina:

- simétrico cuando utiliza la misma clave para cifrar y descifrar;
- asimétrico al usar claves diferentes: una pareja compuesta por una clave pública, que sirve para cifrar, y por una clave privada, que sirve para descifrar. El punto fundamental sobre el que se sostiene esta descomposición pública/privada es la imposibilidad práctica de deducir la clave privada a partir de la clave pública. Este tipo de cifrado suele denominarse PKE (del inglés public-key encription).

Los métodos más conocidos son el DES, el Triple DES y el AES para la criptografía simétrica, y el RSA para la criptografía asimétrica, llamada también criptografía de clave pública.

La utilización de un sistema simétrico o asimétrico depende de las tareas a cumplir. La criptografía asimétrica presenta dos ventajas principales: suprime el problema de transmisión segura de la clave y permite la firma electrónica. No reemplaza sin embargo los sistemas simétricos, ya que los tiempos de cálculo son evidentemente más cortos con los sistemas simétricos que con los asimétricos. (https://definicion.de/cifrado/).

- **ALGORITMO**

  En matemáticas, lógica, ciencias de la computación y disciplinas relacionadas, un algoritmo (del griego y latín, dixit algorithmus y éste a su vez del matemático persa Al-Juarismi) es un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien deba realizar dicha actividad. Dados un estado inicial y una entrada, siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución. Los algoritmos son el objeto de estudio de la algoritmia.

  En la vida cotidiana, se emplean algoritmos frecuentemente para resolver problemas. Algunos ejemplos son los manuales de usuario, que muestran algoritmos para usar un aparato, o las instrucciones que recibe un trabajador por parte de su patrón. Algunos ejemplos en matemática son el algoritmo de multiplicación, para calcular el producto, el algoritmo de la división para calcular el cociente de dos números, el algoritmo de Euclides para obtener el máximo común divisor de dos enteros positivos, o el método de Gauss para resolver un sistema de ecuaciones lineales.

  TIPO DE ALGORITMOS

  - **Tiempo secuencial**. Un algoritmo funciona en tiempo discretizado –paso a paso–, definiendo así una secuencia de estados computacionales por cada entrada válida (la entrada

son los datos que se le suministran al algoritmo antes de comenzar).

- **Estado abstracto**. Cada estado computacional puede ser descrito formalmente utilizando una estructura de primer orden y cada algoritmo es independiente de su implementación (los algoritmos son objetos abstractos) de manera que en un algoritmo las estructuras de primer orden son invariantes bajo isomorfismo.
- **Exploración acotada**. La transición de un estado al siguiente queda completamente determinada por una descripción fija y finita; es decir, entre cada estado y el siguiente solamente se puede tomar en cuenta una cantidad fija y limitada de términos del estado actual.

(Brassard, G.; Bratley, P. (1997). Fundamentos de Algoritmia. Madrid: PRENTICE HALL).

- **LENGUAJE DE PROGRAMACION**

  Un lenguaje de programación es un lenguaje formal diseñado para realizar procesos que pueden ser llevados a cabo por máquinas como las computadoras.

  Pueden usarse para crear programas que controlen el comportamiento físico y lógico de una máquina, para expresar algoritmos con precisión, o como modo de comunicación humana.

  Está formado por un conjunto de símbolos y reglas sintácticas y semánticas que definen su estructura y el significado de sus

elementos y expresiones. Al proceso por el cual se escribe, se prueba, se depura, se compila (de ser necesario) y se mantiene el código fuente de un programa informático se le llama programación. También la palabra programación se define como el proceso de creación de un programa de computadora, mediante la aplicación de procedimientos lógicos, a través de los siguientes pasos:

- El desarrollo lógico del programa para resolver un problema en particular.
- Escritura de la lógica del programa empleando un lenguaje de programación específico (codificación del programa).
- Ensamblaje o compilación del programa hasta convertirlo en lenguaje de máquina.
- Prueba y depuración del programa.
- Desarrollo de la documentación.

(http://conogasi.org/articulos/lenguaje-de-programacion/)

2.3. BASES EPISTÉMOLOGICAS

ENCRIPTACION / DESENCRIPTACION (cifrado)

- El proceso de cifrado/descifrado se establecen una serie de términos y convenios para facilitar referirse a los distintos elementos que intervienen:
- El texto en claro o texto plano (en inglés, plain text) es el mensaje que se cifra.
- El criptograma o texto cifrado es el mensaje resultante una vez que se ha producido el cifrado, es decir, el mensaje cifrado.

- El cifrado es el proceso que consiste en convertir el texto plano en un galimatías ilegible (cifrar), el mensaje cifrado.
- El cifrador es el sistema que implementa el algoritmo de cifrado.
- El algoritmo de cifrado o cifra es el algoritmo que se utiliza para cifrar.
- La clave de cifrado se utiliza en el algoritmo de cifrado.
- El descifrado es el proceso de convertir el texto cifrado en el texto en claro.
- El descifrador es el sistema que implementa el algoritmo de descifrado.
- El algoritmo de descifrado o descifra es el algoritmo que se utiliza para descifrar.
- La clave de descifrado se utiliza en el algoritmo de descifrado.
- La gestión de claves es el proceso de generación, certificación, distribución y cancelación de todas las claves, necesarios para llevar a cabo el cifrado.
- El criptosistema es el conjunto estructurado de los protocolos, los algoritmos de cifrado/descifrado, los procesos de gestión de claves y las actuaciones de los usuarios.
- La descripción de entidades: cuando se desea describir un algoritmo de cifrado/descifrado que involucra el envío de mensajes secretos, muchos autores usan los nombres genéricos Alice y Bob en lugar de los crípticos A y B. Si intervienen otras entidades (C, D, F... -la E quedaría reservada-), se les asignan entonces nombres que empiecen con estas iniciales, y los más frecuentes son Carol y

> Dave. Cuando un escenario involucra protección frente a atacantes que hacen escuchas, entonces para referirse a ellos se suele usar el nombre Eve (del término inglés eavesdropper, "fisgón") o bien el nombre Mallory, en caso de que el atacante, además de interceptar el mensaje, tenga la habilidad de alterarla.

Con frecuencia a los procesos de cifrado y descifrado se les denomina encriptado y desencriptado, ambos anglicismos de los términos ingleses encrypt y decrypt. La Real Academia Española recogió esa acepción en la edición de su diccionario de 2014. Por su parte La Fundación del Español Urgente defiende que encriptar es un término válido y que no hay razón para censurar su uso.

La criptografía en el pasado

En la criptografía clásica los cifrados se basaban en la sustitución (cifrado por sustitución), en la permutación (cifrado por transposición) o en una combinación de ambas técnicas. Habitualmente, las operaciones se aplicaban a bloques aunque otras veces se aplicaban al texto plano completo. Había cifrados por transposición que cambiaban la posición de caracteres a lo largo de la cadena que tenía que cifrarse. Por ejemplo, un cifrado podía consistir en permutar e invertir el orden de los caracteres, dejando el primer carácter en la última posición, el último en la primera posición, el segundo en penúltimo lugar, etcétera.

(http://www.qualityinfosolutions.com/metodos-para-encriptar-y-desencriptar/)

HACKER

Según el diccionario de los hackers, es todo individuo que se dedica a programar de forma entusiasta, o sea un experto entusiasta de cualquier tipo, que considera que poner la información al alcance de todos constituye un extraordinario bien. De acuerdo a Eric Raymond el motivo principal que tienen estas personas para crear software en su tiempo libre, y después distribuirlos de manera gratuita, es el de ser reconocidos por sus iguales. El término hacker nace en la segunda mitad del siglo XX y su origen está ligado con los clubes y laboratorios del MIT.

(http://www.catb.org/jargon/)

En informática, un hacker es una persona que pertenece a una de estas comunidades o subculturas distintas, pero no completamente independientes.

(http://web.archive.org/web/20130116013520/http://webzone.k3.mah.se/k3jolo/HackerCultures/origins.htm)

En seguridad informática este término concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet ("Black hats"). Pero también incluye a aquellos que depuran y arreglan errores en los sistemas ("White hats") y a los de moral ambigua como son los "Grey hats".

Una comunidad de entusiastas programadores y diseñadores de sistemas originada en los sesenta alrededor del Instituto Tecnológico

de Massachusetts (MIT), el Tech Model Railroad Club (TMRC) y el Laboratorio de Inteligencia Artificial del MIT.5 Esta comunidad se caracteriza por el lanzamiento del movimiento de software libre.6 El RFC 13927 amplía este significado como “persona que se disfruta de un conocimiento profundo del funcionamiento interno de un sistema, en particular de computadoras y redes informáticas”.

La comunidad de aficionados a la informática doméstica, centrada en el hardware posterior a los setenta y en el software (juegos de computadora, crackeo de software, la demoscene) de entre los ochenta/noventa. Se utiliza la palabra hacker, para describir a una persona que practica la programación informática, con una especie de pasión artística, o que forma parte de la cultura de los hackers, es decir al grupo de programadores que históricamente están en los orígenes de Internet, en Linux y en la World Wide Web. Desde que se usó por primera vez la palabra hacker ésta ha sido mal utilizada, mal interpretada y encasillada en un contexto errado, antes que nada, aclaremos que el término hacker no tiene nada que ver con actividades delictivas, si bien muchos Hackers cometen errores, la definición no tiene nada que ver con ello.

Definición 1: Término para designar a alguien con talento, conocimiento, inteligencia e ingenio, especialmente relacionada con las operaciones de computadora, redes, seguridad, etc.

Definición 2: Persona que disfruta aprendiendo detalles de los sistemas de programación y cómo extender sus capacidades, tan intensamente

como, al contrario, muchos usuarios prefieren aprender sólo el mínimo necesario.

Definición 3: Persona que es experta en el ámbito de la programación en la utilidad de operaciones de tecnología como: aparatos tecnológicos (computadoras, celulares, etc), redes, seguridad entre otros.

No obstante, más allá de las definiciones del término "Hacker" vinculadas al mundo informático o tecnológico, cabe destacar el uso de esta palabra por extensión (y de hecho así fue en sus inicios el origen de la misma) a toda persona que implementa soluciones para cualquier sistema, sea informático o no, de manera que éste pueda emplearse de formas no pensadas por quienes crearon dichos sistemas. Así mismo, el término Hacker está indisolublemente unido a toda persona que manipula o que posee conocimientos prácticos que modifican los usos de las cosas de modo que éstas puedan emplearse para fines no previstos en su origen. De ahí el uso de los términos de "hackeado" como sinónimo de "alterado en sus fines" para cumplir otras funciones.

También a definición se puede considerar más relevante es que el hacker es la persona que se encarga en encontrar fallos de seguridad para poder resolverlos, y los crackers son los personajes que buscan esos fallos de seguridad para poder beneficiarse de ellos sacando información, vendiendo esos fallos o determinadas cosas.

(https://sites.google.com/site/hackingsistemasinformaticos)

CAPÍTULO III

MARCO METODOLÓGICO

3.1. TIPO DE INVESTIGACIÓN

El tipo de investigación fue **EXPLICATIVA**, porque se utilizaron conocimientos existentes, con la finalidad de analizar el problema y verificar la influencia de los sistemas de cifrado ROCE en la seguridad de los archivos de texto.

Según HERNÁNDEZ SAMPIERI, R., FERNÁNDEZ COLLADO, C., & BAPTISTA LUCIO, P. (2006). En la obra Metodología de la investigación, indica que: los estudios explicativos pretenden establecer las causas de los eventos, sucesos o fenómenos que se estudian. Van más allá de la descripción de conceptos o fenómenos físicos o sociales. Determinan las causas de los fenómenos, Generan un sentido de entendimiento y combinan sus elementos de estudio.

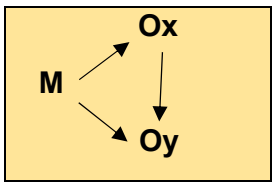
3.2. DISEÑO DE LA INVESTIGACIÓN

La presente investigación fue un estudio de campo ya que los datos fueron recogidos directamente de la realidad a través de la aplicación de una ficha técnica, con la finalidad de analizar el problema y verificar la influencia de los sistemas de cifrado ROCE en la seguridad de los archivos de texto.

Según HERNÁNDEZ SAMPIERI, R., FERNÁNDEZ COLLADO, C., & BAPTISTA LUCIO, P. (2006). En la obra Metodología de la investigación, define que: el diseño de campo es aquel: “Donde los datos se recogen directamente de la realidad, por lo cual los

denominamos primarios, su valor radica en que permiten cerciorarse de las verdaderas condiciones en que se han obtenido los datos, lo cual facilita su revisión o modificación en caso de surgir dudas".

Por su diseño se utilizó la siguiente fórmula:



Donde:

M = Muestra

Ox = Observaciones de la variable influyente

(Sistema de encriptación ROCE)

↓ = Influencia

Oy = Observaciones de la variable influida

(Seguridad de Archivos de Texto)

3.3. POBLACIÓN Y MUESTRA.

- ✓ **POBLACION**

La población de estudio estuvo conformada por los archivos enviados output y recibos input con cifrado ROCE en la zona WIFI de la UNU (Universidad Nacional de Ucayali), hecho por los alumnos, docentes y público en general que hizo uso de los equipos de la Zona WiFi de la UNU.

Los archivos se obtuvieron durante dos (02) meses, de los cuales solo se escogerán aquellos tengan el cifrado ROCE.

TABLA 2. ARCHIVOS CON CIFRADO ROCE ENVIADO/RECIBIDO

ARCHIVOS	CANTIDAD
Grafico	3,451
Texto	**7,890**
Video	730
Audio	1,801
Total	13,872

FUENTE: FORMATO DE TOMA DE DATOS

Siendo nuestra población 7,890 archivos de texto enviado/recibidos por los usuarios en el Laboratorio WiFi-2017.

- ✓ **MUESTRA**

Para calcular el tamaño de la muestra se utilizó la siguiente fórmula:

La cifra que obtuvo, se dio según el error de muestreo y el nivel de confianza.

Si el error de muestreo considerado fue 0.05, el nivel de confiabilidad será del 95%.

Entonces la muestra se obtuvo de la siguiente manera.

$$N = \frac{4.P.Q.N}{4.Q.P + (N-1).E^2}$$

Donde:

X= Tamaño de la muestra.

N= Tamaño de la población

4= Estadístico que prueba al 95% de confianza

E2= Máximo error permisible (5%)

P= Probabilidad de éxito (0,5)

Q= Probabilidad de fracaso (0,5)

$$x = \frac{4 * 0.5 * 0.5 * 7890}{(4 * 0.5 * 0.5) + (7890 - 1) * 0.05 * 0.05}$$

$$x = 381$$

Por tanto, la muestra es de 381 archivos que se hizo transacción de información en la zona WiFi de la UNU.

3.4. INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Utilizamos una ficha técnica, el cual fue estructurado para el ingreso de datos, en forma puntual, de acuerdo al requerimiento de la investigación.

FICHA TECNICA DATO DE ARCHIVOS

PROPIEDADES GENERALES

TIPO	**TEXTO**	
	IMAGEN	
	AUDIO	
	VIDEO	
	OTROS	
UBICACIÓN	**DISCO DURO**	
	CD / DVD/BRD	
	MEMORIA EXERNA	
	EN LA NUBE	
TAMAÑO		

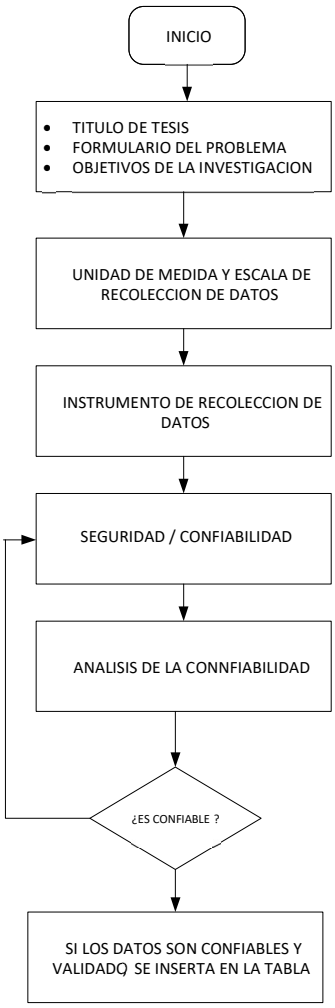
SEGURIDAD

TIPO DE ENCRIPTACION	**ROCE**	
	RSA	
	DES	
	WAP	
	PSK	
	AES	
	PGP	
SOFTWARE DE ENCRIPTACION	**Steganos Safe**	
	AxCrypt	
	ENIGMA	
	Gpg4win	
	DiskCryptor	
	7.Zip	

VALIDACION Y CONFIABILIDAD DEL INSTRUMENTO ESTADISTICO

Hidalgo, L. 2005. En la obra, Confiabilidad y Validez en el Contexto de la Investigación y Evaluación Cualitativas, indica que: …La validez y confiabilidad son: "constructos" inherentes a la investigación, desde la perspectiva positivista, con el fin de otorgarle a los instrumentos y a la información recabada, exactitud y consistencia necesarias para efectuar las generalizaciones de los hallazgos, derivadas del análisis de las variables en estudio"

DISEÑO DE LA VALIDACION Y CONFIABILIDAD DEL INSTRUMENTO ESTADISTICO



Para determinar la validez y confiabilidad se desarrolló a través del juicio de expertos, haciendo la consulta a tres docentes con el grado de magister, tal como se demuestra en el Anexo 03, alcanzado una Valoración Cuantitativa de 18.00 puntos (aceptable), por lo tanto nuestro instrumento queda validado, los resultados fueron aplicados en una escala de 0 – 20 puntos, de acuerdo al siguiente formato que se puede apreciar en el **Anexo 03.**

DATOS DE LOS EXPERTOS

Mg. David León Moreno
Universidad Nacional de Ucayali

Mg. Cesar Augusto Agurto Cherre
Universidad Nacional de Ucayali

MSc. Milton Miguel Pirro Lozano
Universidad Nacional de Ucayali

3.5. TÉCNICAS DE RECOJO, PROCESAMIENTO Y PRESENTACIÓN DE DATOS.

Los resultados son presentados en tablas y gráficos, analizados con la aplicación de la estadística descriptiva.

- Para el procesamiento de los datos se utilizaron las herramientas informáticas como: Ms Excel y el Ms Process, presentándose los resultados en cuadros de doble entrada y gráficos respectivos, teniendo en cuenta las variables de la investigación.
- El Análisis Estadístico nos permitió elaborar los cuadros estadísticos, para obtener un mejor análisis de la información que se ha obtenido de nuestras encuestas, entrevistas y otros datos obtenidos durante la ejecución del proyecto de investigación.

CAPÍTULO IV

RESULTADOS

4.1. RECOLECCIÓN, PRESENTACIÓN Y TRATAMIENTO DE DATOS

Los resultados son presentados en tablas y gráficos, analizados con la aplicación de la estadística descriptiva, seguidamente se procedió a analizar las características de cada uno de los datos de las variables.

Para el procesamiento de los datos se utilizaron las herramientas informáticas como: Ms Excel y Ms Process, presentándose los resultados en cuadros de doble entrada y gráficos respectivos, teniendo en cuenta las variables de la investigación.

4.2. PRESENTACIÓN DE RESULTADOS

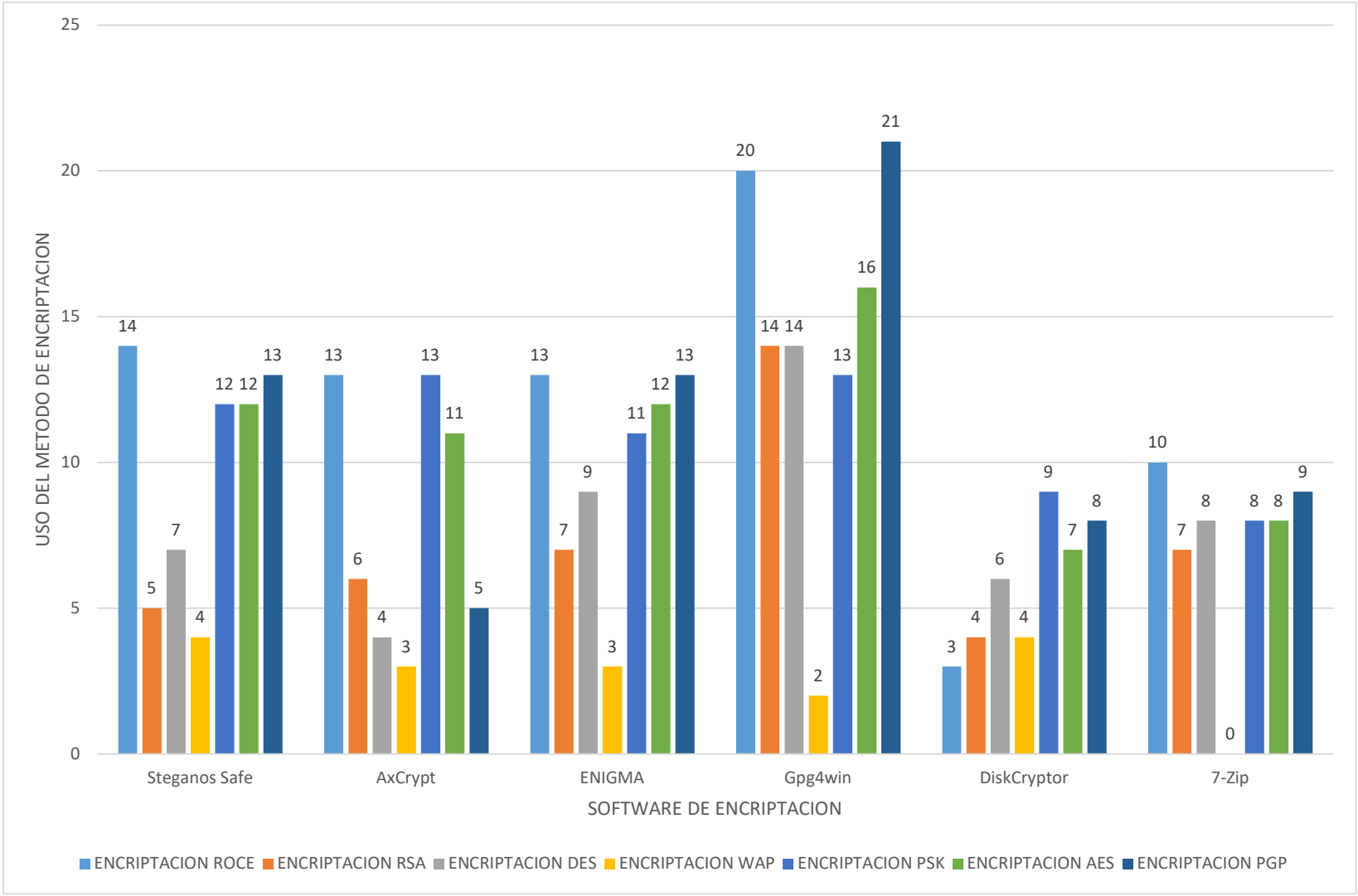
El objetivo del estudio, de acuerdo a Pardinas (1985) comprobar la operatividad, duración, fidelidad y validez del instrumento. Asimismo, de acuerdo a Alarcón (1991) se señala que el estudio se realiza con dos propósitos: determinar si los formularios recogen la información necesaria y en qué medida el formulario va a contribuir a ofrecer una buena relación con el usuario, en este caso con los estudiantes que hacen uso del Laboratorio Wifi para el envío y recepción de datos.

TABLA 3. METODO DE ENCRIPTACION SEGÚN SOFTWARE UTILIZADO

		SOFTWARE DE ENCRIPTACION					
		Steganos Safe	**AxCrypt**	**ENIGMA**	**Gpg4win**	**DiskCryptor**	**7-Zip**
ENCRIPTACION	**ROCE**	**14**	13	13	20	3	10
	RSA	**5**	6	7	14	4	7
	DES	**7**	4	9	14	6	8
	WAP	**4**	3	3	2	4	0
	PSK	**12**	13	11	13	9	8
	AES	**12**	11	12	16	7	8
	PGP	13	5	13	21	8	9

FUENTE: FICHAS DE RECOLECCION DE DATOS -2017

GRÁFICO 1. METODO DE ENCRIPTACION SEGÚN SOFTWARE UTILIZADO



INTERPRETACION PARCIAL

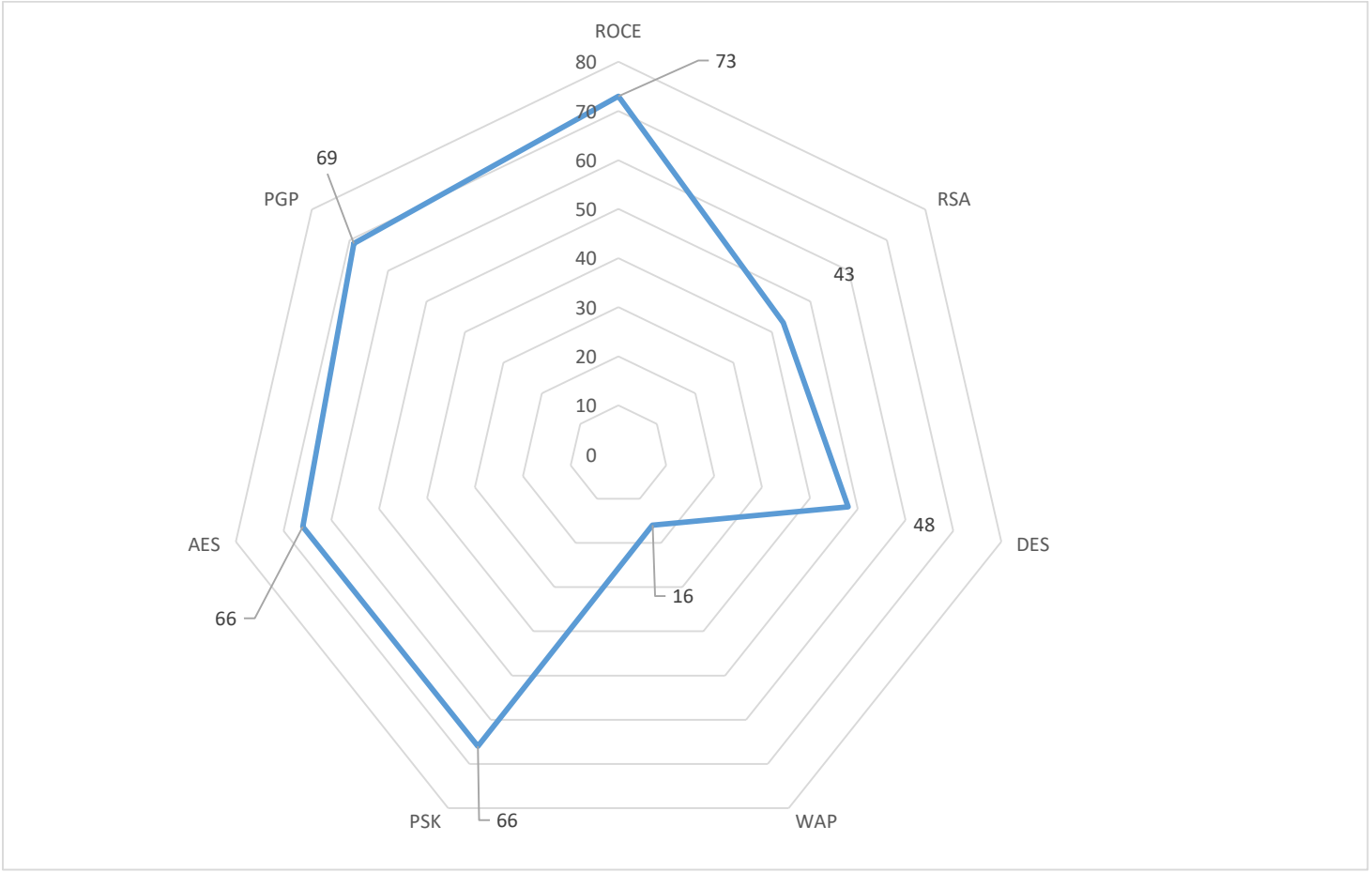
- El software de encriptación más usado es Gpg4Win, con un 26.2% (100 veces usado), siguiendo ENIGMA con 17.8 % (68 veces) y Steganos Safe con 17.6% (67 veces), podemos afirmar que el uso de Gpg4win se da como primer lugar por ser el más usado por la mayoría de empresas dedicados a ciberseguridad, mientras que ENIGAMA, lo hacen por un entorno más comercial.

TABLA 4. METODO DE ENCRIPTADO USADO

METODO DE ENCRIPTACION	CANTIDAD
ROCE	73
RSA	43
DES	48
WAP	16
PSK	66
AES	66
PGP	69
TOTAL	381

FUENTE: FICHAS DE RECOLECCION DE DATOS -2017

GRÁFICO 2. METODO DE ENCRIPTADO USADO



INTERPRETACION PARCIAL

- Del total de algoritmos analizados, el algoritmo más usado en este estudio fue el ROCE con un 19.2 % (73 veces), PGP con un 18.1% (69 veces) y 17.3% (66 veces) tanto PSK y AES.

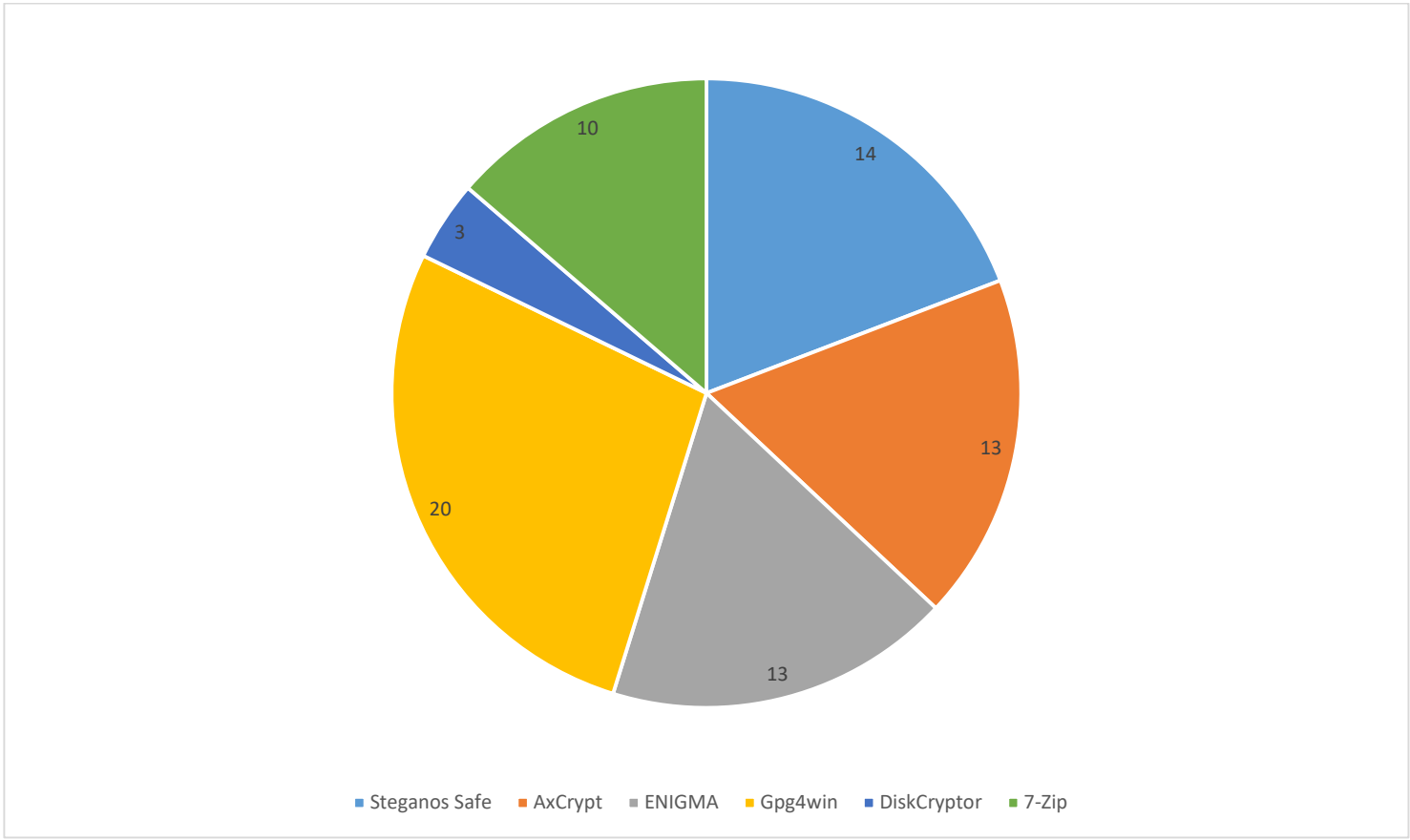
4.3. VERIFICACION DE LA HIPOTESIS

TABLA 5. USO DEL ROCE POR VS SOFTWARE DE ENCRIPTACION

SOFTWARE DE ENCRIPTACION	NRO DE VECES
Steganos Safe	14
AxCrypt	13
ENIGMA	13
Gpg4win	20
DiskCryptor	3
7-Zip	10
TOTAL	73

FUENTE: FICHAS DE RECOLECCION DE DATOS -2017

GRÁFICO 3. USO DEL ROCE VS SOFTWARE DE ENCRIPTACION



INTERPRETACION PARCIAL

Del 100% del uso del algoritmo ROCE por los softwares de encriptación, se aprecia que Gpg4win es usado en 27.4% (20 veces) por ser el software de encriptación que se aplica en la transacción de datos por las empresas de ciberseguridad, mientras que se aprecia que Steganos Safe lo usan en un 19.2% (14 veces), tanto AxCrypt y ENIGMA lo usaron en un 17.8% (13 veces).

ANALISIS COMPARATIVO DEL USO DEL ALGORITMO ROCE EN LA SEGURIDAD DE LOS ARCHIVOS DE TEXTO.

Del 100% del uso del algoritmo ROCE por los softwares de encriptación, se aprecia que Gpg4win es usado en 27.4% (20 veces) por ser el software de encriptación que se aplica en la transacción de datos por las empresas de cyberseguridad, mientras que se aprecia que Steganos Safe lo usan en un 19.2% (14 veces), tanto AxCrypt y ENIGMA lo usaron en un 17.8% (13 veces).

Por lo que podemos afirmar que al hacer uso de un algoritmo de encriptación para dar seguridad de datos tipo texto, se usa el ROCE en un alto porcentaje, así mismo ninguno de los usuarios del laboratorio WiFi nos informó que tuvieron problemas en el envío o recepción de información.

CAPÍTULO V

DISCUSIÓN DE RESULTADOS

En este capítulo presentamos la confrontación de la situación problemática formulada con los referentes bibliográficos, la hipótesis general en base a la prueba de hipótesis y el aporte científico de la investigación.

5.1. CONTRASTACIÓN DE LOS RESULTADOS DEL TRABAJO DE CAMPO CON LOS REFERENTES BIBLIOGRÁFICOS DE LAS BASES TEÓRICAS.

Luego de haber concluido con la investigación y a la luz de los resultados obtenidos se pudo determinar que de los sistemas de encriptación Roce influye significativamente en la seguridad de archivos de texto, tal como se demuestra en la TABLA 3: METODO DE ENCRIPTACION SEGÚN SOFTWARE UTILIZADO y en la TABLA 3: METODO DE ENCRIPTADO USADO EN EL ENVIO DE ARCHIVOS DE TEXTO.

Leon K. (2015) indica que: “Los algoritmos de encriptación tienen una base fuertemente matemática y de esto no escapa el RSA, poder manejar estos conceptos dentro de este programa no ha sido precisamente de las tareas más sencillas, sino por el contrario demandó mucho tiempo no solo en entender el funcionamiento del algoritmo sino también en la implementación y pruebas del mismo.”

5.2. PRESENTAR LA CONTRASTACIÓN DE LA HIPÓTESIS GENERAL EN BASE A LA PRUEBA DE HIPÓTESIS.

Al finalizar el presente trabajo de investigación, se observa en la TABLA 4: USO DEL ROCE POR VS SOFTWARE DE ENCRIPTACION, que al hacer uso de un algoritmo de encriptación para dar seguridad de datos tipo texto, se usa el ROCE en un alto porcentaje, llegando a un 27.4% (20 veces) así mismo ninguno de los usuarios del laboratorio wifi, informó que tuvieron problemas en el envió o recepción de información.

5.3. PRESENTAR EL APORTE CIENTÍFICO DE LA INVESTIGACIÓN

El resultado y producto de nuestra investigación tiene una importancia teórico científico, pues se trata de una contribución al desarrollo de la ciencia en la computación. Los sistemas de encriptación se aplican en toda transacción de información, y es aplicado por todo software de comunicación bajo el modelo predefinido con un estándar de seguridad intermedio, por lo regular el usuario no necesita configurar el nivel de seguridad, pero si este requiere elevar la seguridad, lo puede hacer, esta decisión tiene como requisitos tener conocimientos de encriptación, entendiendo que el tiempo de demora será mayor.

De la investigación desarrollada podemos ver que hasta la investigación desarrollada el algoritmo ROCE es usado casi en todos los softwares de encriptación en un alto porcentaje, se aprecia que Gpg4win lo usa e 27.4% (20 veces) mientras que Steganos Safe lo usan en un 19.2% (14 veces), y tanto AxCrypt y ENIGMA lo usaron en un 17.8% (13 veces).

CONCLUSIONES.

- Se ha podido determinar la influencia de los sistemas de cifrado ROCE en la seguridad de los archivos de texto, tal como se ha podido demostrar en tabla 3, donde el algoritmo de encriptación es el ROCE, alcanzado un 19.2% de los algoritmos más usados, con 73 veces en el estudio utilizado.
- Se ha podido identificar el grado de asociación entre el uso cifrado Roce y la seguridad de archivos tipo texto es alta tal como se puede ver la tabla 1, siendo el software de encriptación Gpgwin el más usado con un 27.4% con (20 veces), con el algoritmo ROCE.
- Se ha podido conocer los resultados del uso de los sistemas de cifrado ROCE en la seguridad de archivos de texto, siendo uno de los más usados, agrupándose en dos softwares de encriptación: Gpgwin y Steganos Safe alcanzado en conjunto 46.6% su uso, como se ha podido ver en la tabla 5.

SUGERENCIAS.

- Es necesario seguir profundizando los estudios sobre seguridad de archivos en lo que concierne a encriptación, en donde se determine las regularidades fundamentales que permitan determinar un mejor nivel de seguridad. El autor considera, la importancia de continuar desarrollando procesos de autoevaluación y evaluación de los algoritmos que generan eficiencia en las transacciones de archivos, para lograr un estado de perfeccionamiento, calidad en la seguridad de las transacciones.

- De las conclusiones alcanzadas en la presente investigación se sugiere que al momento de realizar las transacciones de información las cuales son valiosas para usted, no solo debe elegir la mejor seguridad para su información sino también el costo computacional para tal fin; algunos algoritmos de seguridad tienen costos de procesamiento muy altos, esto hace que se demore más tiempo en encriptar o desencriptar.

BIBLIOGRÁFIA

- Boneh, D., Franklin M. 2001. “Identity-based Encryption from the Weil pairing”. En Advances in Cryptology: Proceedings of CRYPTO ’01. Santa Bárbara, USA. International Associaton for Cryptograhpic Research. Springer.
- Brassard, G.; Bratley, P. (1997). Fundamentos de Algoritmia. Madrid: PRENTICE HALL
- Bunge, Mario. La investigación científica. España: Editorial Ariel, 1997
- Chatterjee, S., Sakar, P. 2009. “Identity Based Encription and Hierarchical Identity Based Encription” En: JOYE, M., NEVEN, G. Identity-Based Cryptography, Vol 2. Países Bajos,
- Day, Robert. Cómo escribir y publicar trabajos científicos. Tercera edición. Washington, EUA: Organización Panamericana de la Salud, 2005.
- Gates Rubber de México. Catalogo Master De Bandas Industriales Transmisión De Potencia. Gates, 2000.
- Hidalgo, L. 2005. En la obra, Confiabilidad y Validez en el Contexto de la Investigación y Evaluación Cualitativas
- León K. (2005), Pontificia Universidad Catolica Del Peru, Escuela De Graduados, Encriptacion Rsa, De Archivos De Texto
- MORENO M. (2010) Universidad De Chile, Diseño E Implementación De Un Esquema De Encriptación Y Firmas Basado En Identidad Ara Dispositivos Bug.
- Reyes R. R., Soto M. L. E. Metodología para el Desarrolla de Proyectos de Ingeniería. Editorial Bramvila, México 2007.

- Senge, Peter. La quinta disciplina. El arte y la práctica de la organización abierta al aprendizaje. España: Graniza. 1998
- SOTO J.(2010), Instituto Politecnico Nacional De Mexico, Algoritmo De Encriptacion Simétrico Qe Procesa Bloques De 192 Bits, Con Llaves De Cifrado De 192 Bits, Empleando Los Teoremas Factorial Y Jv
- Unesco. Guía para la redacción de artículos científicos destinados a la publicación. 2 ed, París: UNESCO, 1983
- G.E.P. Box, W.G. Hunter, J.S. Hunter. *Estadística para experimentadores*. Ed. Reverté. Barcelona, 1989.
- Robert. Sampieri, Carlos Fernández, María Batista. *"Metodología de la Investigación"* Quinta Edición Mc Graw – Hill Interamericana Editores, S.A. de C.V.

ANEXOS

ANEXO: 01 – MATRIZ DE CONSISTENCIA

TITULO "LOS SISTEMAS DE CIFRADO ROCE EN LA SEGURIDAD DE ARCHIVOS DE TEXTO"							
FORMULACION DEL PROBLEMA	**OBJETIVOS**	**HIPOTESIS**	**VARIABLES**	**DIMENCIONES**	**INDICADORES**	**INSTRUMENTO**	**METODOLOGIA**
FORMULACIÓN DEL PROBLEMA GENERAL En qué medida el uso del cifrado ROCE, ayuda en la seguridad de archivos de texto **PROBLEMAS ESPECÍFICOS** • ¿Cuál es el grado de asociación entre el uso de cifrado Roce y la Seguridad Tipo Texto? • ¿Cuáles Son los resultados del uso de los sistemas de cifrado Roce en la seguridad de archivos de texto?.	**OBJETIVO GENERAL** Determinar la influencia de los sistemas de cifrado ROCE en la seguridad de los archivos de texto **OBJETIVOS ESPECÍFICOS** • Identificar el grado de asociación entre el uso cifrado Roce y la seguridad de archivos tipo texto. • Conocer los resultados del uso de los sistemas de cifrado Roce en la seguridad de archivos de texto.	**HIPÓTESIS GENERAL** La aplicación de los sistemas de encriptación Roce influye significativamente en la seguridad de archivos de texto. **HIPÓTESIS NULA:** La Aplicación de los sistemas de encriptación ROCE no influye significativamente en la seguridad de archivos de texto. **HIPÓTESIS SECUNDARIAS** • El grado de asociación entre el uso cifrado Roce y la seguridad de archivos tipo texto es alta. • El uso de los sistemas de cifrado Roce en la seguridad de archivos de texto tiene un alto porcentaje de uso.	**Variable Independiente** Sistemas de cifrado ROCE **Variable Independiente** Seguridad de archivos de texto **Variable Interviniente** Universidad Nacional de Ucayali	Algoritmo Protección	• Eficiencia • Efectividad • Nivel de seguridad • Portabilidad	**Ficha de recojo de datos**	**Tipo De Investigación** será aplicada, porque se utilizarán conocimientos existentes, con la finalidad de analizar el problema y verificar influencia de los sistemas de cifrado ROCE en la seguridad de los archivos de texto **Diseño y esquema de la investigación.** El nivel de investigación será Descriptiva, porque nos ayudará a recolectar los datos necesarios de hechos, eventos y situaciones ocurridos, y se tratarán de medir estos eventos con la máxima precisión. **Población** estará conformada por los archivos enviados output y recibos input con cifrado ROCE en la zona wifi de la Universidad Nacional de Ucayali **Muestra** Para calcular el tamaño de la muestra se utilizara la siguiente fórmula: $n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}$ **TECNICAS A USAR** Ficha

ANEXO: 02 - FICHA TECNICA DATO DE ARCHIVOS

RECOMENDACIONES: MARQUE CON UNA "X" EN EL CUADRO QUE CORRESPONDA, O RELLENE CON LOS DATOS QUE SE SOLICITA.

PROPIEDADES GENERALES

TIPO	**TEXTO**	
	IMAGEN	
	AUDIO	
	VIDEO	
	OTROS	
UBICACIÓN	**DISCO DURO**	
	CD / DVD/BRD	
	MEMORIA EXERNA	
	EN LA NUBE	
TAMAÑO		

SEGURIDAD

TIPO DE ENCRIPTACION	**ROCE**	
	RSA	
	DES	
	WAP	
	PSK	
	AES	
	PGP	
SOFTWARE DE ENCRIPTACION	**Steganos Safe**	
	AxCrypt	
	ENIGMA	
	Gpg4win	
	DiskCryptor	
	7.Zip	

ANEXO: 03 - VALIDACION DEL INSTRUMENTO POR JUICIO DE EXPERTOS

VALIDACIÓN DEL INSTRUMENTO POR EXPERTOS

I. DATOS PERSONALES:

1.1. APELLIDO Y NOMBRE DEL INFORMANTE:
Meza Marcos David

1.2. GRADO ACADÉMICO:
MAGISTER

1.3. INSTITUCIÓN DONDE LABORA:
UNU

1.4. TITULO DE INVESTIGACIÓN:
LOS SISTEMAS DE CIFRADO ROCE EN LA SEGURIDAD DE ARCHIVOS DE TEXTO

1.5. AUTOR DEL INSTRUMENTO:
YUMI TOMINAGA GARCIA

1.6. NOMBRE DEL INSTRUMENTO:
FICHA TECNICA

II. ASPECTOS A EVUALAR: (CALIFICACIÓN CUANTITATIVA)

INDICADORES DEL INSTRUMENTO DE EVALUACIÓN	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-13)	Bueno (14-16)	Muy bueno (17-18)	Excelente (19-20)
01 CLARIDAD					/	
02 OBJETIVIDAD					/	
03 ACTUALIDAD					/	
04 ORGANIZACIÓN					/	
05 SUFICIENCIA					/	
06 INTENCIONALIDAD					/	
07 CONSISTENCIA					/	
08 COHERENCIA					/	
09 METODOLOGÍA					/	
10 OPORTUNIDAD					/	
SUB TOTAL					180	
TOTAL						18

VALORACION CUANTITAVA (TOTAL XO,4): 18

VALORACION CUALITAVA: Aceptable

VALORACION APLICADA: Aplicar

LEYENDA

01-13 Improcedente.

14-15 aceptable con recomendación.

17-20 aceptable.

Lugar y fecha: Pucallpa, 15/08/18

Firma Y Post –Firma Del Experto:

D.N.I. 22520055

VALIDACIÓN DEL INSTRUMENTO POR EXPERTOS

I. DATOS PERSONALES:

1.1. APELLIDO Y NOMBRE DEL INFORMANTE:
Cesar Augusto Agurto Chevez

1.2. GRADO ACADÉMICO:
Magister

1.3. INSTITUCIÓN DONDE LABORA:
UNU

1.4. TITULO DE INVESTIGACIÓN:
LOS SISTEMAS DE CIFRADO ROCE EN LA SEGURIDAD DE ARCHIVOS DE TEXTO

1.5. AUTOR DEL INSTRUMENTO:
YUMI TOMINAGA GARCIA

1.6. NOMBRE DEL INSTRUMENTO:
FICHA TECNICA

II. ASPECTOS A EVUALAR: (CALIFICACIÓN CUANTITATIVA)

INDICADORES DEL INSTRUMENTO DE EVALUACIÓN	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-13)	Bueno (14-16)	Muy bueno (17-18)	Excelente (19-20)
01 CLARIDAD					X	
02 OBJETIVIDAD					X	
03 ACTUALIDAD					X	
04 ORGANIZACIÓN					X	
05 SUFICIENCIA					X	
06 INTENCIONALIDAD					X	
07 CONSISTENCIA					X	
08 COHERENCIA					X	
09 METODOLOGÍA					X	
10 OPORTUNIDAD					X	
SUB TOTAL					180	
TOTAL						18

VALORACION CUANTITAVA (TOTAL XO,4): 18

VALORACION CUALITAVA: Aceptable

VALORACION APLICADA: Aplicar

LEYENDA

01-13 Improcedente.

14-15 aceptable con recomendación.

17-20 aceptable.

Lugar y fecha... Pucallpa, 17/08/18

Firma Y Post –Firma Del Experto:

D.N.I. 18190341

VALIDACIÓN DEL INSTRUMENTO POR EXPERTOS

I. DATOS PERSONALES:

1.1. APELLIDO Y NOMBRE DEL INFORMANTE:
MILTON MIGUEL PIRRO LOZANO

1.2. GRADO ACADÉMICO:
MAGISTER SCIENTIAE

1.3. INSTITUCIÓN DONDE LABORA:
U.N.U.

1.4. TITULO DE INVESTIGACIÓN:
LOS SISTEMAS DE CIFRADO ROCE EN LA SEGURIDAD DE ARCHIVOS DE TEXTO

1.5. AUTOR DEL INSTRUMENTO:
YUMI TOMINAGA GARCIA

1.6. NOMBRE DEL INSTRUMENTO:
FICHA TECNICA

II. ASPECTOS A EVUALAR: (CALIFICACIÓN CUANTITATIVA)

INDICADORES DEL INSTRUMENTO DE EVALUACIÓN	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-13)	Bueno (14-16)	Muy bueno (17-18)	Excelente (19-20)
01 CLARIDAD					X	
02 OBJETIVIDAD					X	
03 ACTUALIDAD					X	
04 ORGANIZACIÓN					X	
05 SUFICIENCIA					X	
06 INTENCIONALIDAD					X	
07 CONSISTENCIA					X	
08 COHERENCIA					X	
09 METODOLOGÍA					X	
10 OPORTUNIDAD					X	
SUB TOTAL					180	
TOTAL						18

VALORACION CUANTITAVA (TOTAL XO,4): 18

VALORACION CUALITAVA: ACEPTADO

VALORACION APLICADA: APLICAR

LEYENDA

01-13 Improcedente.

14-15 aceptable con recomendación.

17-20 aceptable.

Lugar y fecha: PUCALLPA, 25/08/2018

Firma Y Post –Firma Del Experto:

D.N.I. 00126540