



UNIVERSIDAD TECNOLÓGICA ISRAEL
ESCUELA DE POSTGRADOS

**MAESTRÍA EN TELEMÁTICA,
MENCIÓN: CALIDAD EN EL SERVICIO**
(Aprobado por: RPC-SO-19-No.300-2016-CES)

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título:
Análisis de tecnologías criptográficas, 3DES y RSA, basado en las Normas ISO 27001, para garantizar la integridad de datos en la capa de Transporte con dispositivos Raspberry PI.
Autor/a:
Ing. Camacho Reina Gregorio Aurelio
Tutor/a:
Ing. Vivanco Herrera Henry Rodrigo, Mg.

Quito-Ecuador

2019

AGRADECIMIENTO

Mi eterno agradecimiento a:

Jehová por permitirme llegar hasta este punto de mi vida.

Mi esposa *María*, por acompañarme incondicionalmente.

Mi hijo *Luis*, por ser mi fuente de inspiración.

Mi madre *Consuelo*, por estar presente cuando la necesito.

DEDICATORIA

A mi familia.

Esta línea, materializa un sueño.

Cuando se desea, trabajando mucho, se puede.

ÍNDICE DE CONTENIDOS

AGRADECIMIENTO	i
DEDICATORIA	ii
ÍNDICE DE CONTENIDOS	iii
ÍNDICE DE FIGURAS	ix
ÍNDICE DE ECUACIONES	xiii
ÍNDICE DE ANEXOS	xiv
RESUMEN	xv
ABSTRACT	xvi
Introducción.....	1
Situación Problemática.....	2
Objeto de estudio.....	3
Campo de investigación	3
Objetivo General.	4
Objetivos Específicos.....	4
Justificación de la Investigación	4
CAPÍTULO I.....	5
1.1. Antecedentes Investigativos	5

1.2.	Redes Inalámbricas	6
1.2.1.	WAN	6
1.2.2.	LAN.....	6
1.2.3.	WLAN.....	7
1.3.	Dispositivos Electrónicos	7
1.3.1.	Raspberry PI.....	8
1.3.2.	Arduino	9
1.3.3.	Conexión Wireless	13
1.4.	Sistemas Operativos de código abierto	13
1.4.1.	Linux	13
1.4.2.	Debian	14
1.5.	Software Analizador de Protocolos.....	14
1.5.1.	Wireshark	15
1.5.2.	Nagios	15
1.5.3.	Netflow.....	16
1.6.	Arquitectura SBC (Computadores de Placa Reducida).....	17
1.6.1.	Aplicaciones.....	17
1.6.2.	Redes WSN (Industria)	18
1.6.3.	Domótica	20

1.7.	Seguridad de la Información	21
1.8.	Algoritmos de Cifrado.....	21
1.8.1.	3DES	21
1.8.2.	Rivest, Shamir y Adleman (RSA)	23
1.9.	Normas y Estándares.....	26
1.9.1.	Normas ISO.....	27
1.9.2.	ISO / IEC 27001	27
1.9.3.	ISO / IEC 27002.....	28
CAPÍTULO II.....		29
2.1.	Metodología Investigativa.....	29
2.1.1.	Investigación Descriptiva.....	29
2.1.2.	Diseño Experimental	29
2.1.3.	Enfoque Cuantitativa.....	30
2.2.	Población y muestra	30
2.2.1.	Población.....	31
2.2.2.	Muestra.....	31
2.3.	Métodos y técnicas empleadas para la recolección de la información	35
2.3.1.	Variables.....	35

2.3.2.	Constantes	36
2.3.3.	Parámetros	37
2.4.	Procesamiento de la información	38
2.4.1.	Recolección de la Información.....	41
2.5.	Metodología Aplicada.....	41
2.6.	Herramientas y Materiales	41
CAPÍTULO III		42
3.1.	Fundamentos del proyecto	42
3.2.	Presentación del proyecto.....	42
3.2.1.	Plataforma Tecnológica.....	43
3.2.2.	Planimetría Zonal	43
3.2.3.	Archivo enviado desde Dispositivos Raspberry PI	45
3.2.4.	Analizador de Protocolos	46
3.2.4.1.	Análisis del archivo en texto cifrado	46
3.2.5.	Políticas de Seguridad	48
3.3.	Análisis Comparativo entre Tecnologías de cifrado	53
3.3.1.	Tamaño del archivo	54
3.3.2.	Tiempo de Carga de Archivo	56

3.3.3.	Zona Norte 1.....	56
3.3.4.	Zona Norte 2.....	60
3.3.5.	Zona Centro 1.....	66
3.3.6.	Zona Centro 2.....	71
3.3.7.	Zona Sur 1	76
3.3.8.	Zona Sur 2	79
3.3.9.	Resumen de tiempos de carga al repositorio	81
4.	Conclusiones.....	83
5.	Recomendaciones	85
6.	Bibliografía.....	86
7.	Anexos.....	89
7.1.	Anexo 1. Ficha de Observación	89
7.2.	Anexo 2. Políticas de Seguridad	90
1.	Introducción	90
2.	Objetivo.....	90
3.	Alcance.....	90
4.	Política.....	90
4.1	Claves secretas para cifrado simétrico	91

4.2 Llaves de cifrado de PKI.....	91
4.3 Números de Identificación Personal (PIN), Contraseñas y Pass frases.....	92
4.4 Pérdida y Robo.....	92
5. Cumplimiento de la política.....	92
5.3 Incumplimiento.....	92
6. Procesos y estándares relacionados.....	92
7. Temimos y definiciones.....	93

ÍNDICE DE FIGURAS

Figura 1. Raspberry Pi3, Cara superior	8
Figura 2. Modelo de funcionamiento del cifrado Simétrico.....	22
Figura 3. Funcionamiento del algoritmo de cifrado Triple Des	23
Figura 4. Modelo de funcionamiento del algoritmo asimétrico.	24
Figura 5. Relaciones Estándar ISO 27001 con otras ISO de la misma familia.	27
Figura 6. Organización estructural de los establecimientos	30
Figura 7. Archivo enviado en texto plano.	38
Figura 8. Captura de trama con Wireshark al archivo en texto plano.	39
Figura 9. Datos de usuario.....	39
Figura 10. Datos de usuario.....	40
Figura 11. Formulario de acceso al Repositorio Central.....	40
Figura 12. Mapa de Planimetría Zonal.....	44
Figura 13. Archivo de texto cifrado con 3 DES	45
Figura 14. Archivo de texto cifrado con RSA.....	46
Figura 15. Captura con Wireshark del archivo cifrado con 3DES.	47
Figura 16. Ejemplo de página cifrada con AES y RSA	48
Figura 17. Configuración del Generador de Contraseñas Seguras de KeyPass	52

Figura 18. Pantalla de Gestión de Contraseñas con KeyPass.....	53
Figura 19. Resultado de prueba de tamaño de archivo.....	54
Figura 20. Tamaños de Archivo en Texto Plano y Cifrado.....	55
Figura 21. Resultados de tiempo de carga Host N° 1	57
Figura 22. Resultados de tiempo de carga Host N° 2	57
Figura 23. Resultados de tiempo de carga Host N° 3	58
Figura 24. Resultados de tiempo de carga Host N° 4	58
Figura 25. Resumen Tabla N° 8 de Zona Norte 1	60
Figura 26. Resultados de tiempo de carga Host N° 1	61
Figura 27. Resultados de tiempo de carga Host N° 2	61
Figura 28. Resultados de tiempo de carga Host N° 3	62
Figura 29. Resultados de tiempo de carga Host N° 4	62
Figura 30. Resultados de tiempo de carga Host N° 5	63
Figura 31. Resumen Tabla N° 9 de Zona Norte 2	65
Figura 32. Resultados de tiempo de carga Host N° 1	66
Figura 33. Resultados de tiempo de carga Host N° 2	66
Figura 34. Resultados de tiempo de carga Host N° 3	67
Figura 35. Resultados de tiempo de carga Host N° 4	67

Figura 36. Resultados de tiempo de carga Host N°5	68
Figura 37. Resultados de tiempo de carga Host N° 6	68
Figura 38. Resumen Tabla N° 10 de Zona Centro 1.....	70
Figura 39. Resultados de tiempo de carga Host N° 1	71
Figura 40. Resultados de tiempo de carga Host N° 2	71
Figura 41. Resultados de tiempo de carga Host N° 3	72
Figura 42. Resultados de tiempo de carga Host N° 4	72
Figura 44. Resultados de tiempo de carga Host N° 6	73
Figura 45. Resumen Tabla N° 11 de Zona Norte 2	75
Figura 46. Resultados de tiempo de carga Host N° 1	76
Figura 47. Resultados de tiempo de carga Host N° 2	76
Figura 48. Resultados de tiempo de carga Host N° 3	77
Figura 49. Resumen Tabla N° 12 de Zona Sur 1	78
Figura 50. Resultados de tiempo de carga Host N°1	79
Figura 51. Grafica de Tabla N° 12 de Zona Sur 2.....	79
Figura 52. Resumen Tabla N° 13 de Zona Sur 2.....	80
Figura 53. Resumen Tabla N° 14 de Tiempos de Carga de Archivo.....	82

ÍNDICE DE TABLAS

Tabla 1. Especificaciones técnicas de placas Arduino.....	11
Tabla 2. Población de host	31
Tabla 3. Cuadro de distribución de muestras.....	34
Tabla 4. Variables	35
Tabla 5. Constantes	36
Tabla 6. Parámetros.....	37
Tabla 7 Tamaño del archivos transmitido al Repositorio.....	55
Tabla 8. Zona Norte 1	59
Tabla 9. Zona Norte 2.	64
Tabla 10. Zona Centro 1.....	69
Tabla 11. Zona Centro 2.....	74
Tabla 12. Zona Sur 1	78
Tabla 13. Zona Sur 2.....	79
Tabla 14. Resumido de Tiempos de Carga del archivo al Repositorio.....	81

ÍNDICE DE ECUACIONES

Ecuación 1 Fórmula para determinar la población total.....	32
Ecuación 2. Muestra Estratificada.....	32
Ecuación 3. Constante k.....	33
Ecuación 4. Valor de constante k.....	33
Ecuación 5. Coeficiente de Ponderación.....	33
Ecuación 6. Calculo de la Muestra Proporcional	33
Ecuación 7. Calculo para encontrar cada muestra proporcional del universo poblacional	34

ÍNDICE DE ANEXOS

Anexo 1. Ficha de Observación	89
Anexo 2. Políticas de Seguridad.....	90

RESUMEN

Con los avances en las tecnologías, cada vez son más los procesos que son automatizados y la centralización de la información se convierte en una necesidad, por lo que el transporte de la información debe realizarse de una manera segura y rápida, siendo necesario utilizar mecanismos que apoyen este primer factor, y uno de ellos es la criptografía.

Existen más de un mecanismo criptográfico que puede utilizarse para brindar seguridad a la información, utilizando diferentes plataformas y software, pero muy poco sobre investigaciones en plataformas con dispositivos de placa única.

Por las características limitadas propias de los microordenadores de placa única, se vuelve necesario realizar la presente investigación, los dispositivos como Raspberry, por su bajo costo, fácil mantenimiento, tamaño reducido y gran resistencia a factores de deterioro como el clima, la humedad, el polvo, incluso ataques de insectos, son ventajas que ofrecen el uso de este tipo de dispositivos para las empresas agrícolas especialmente.

Encontrar un algoritmo que brinde la seguridad necesaria, sin provocar un desmayo en el funcionamiento del dispositivo provocado por la carga de trabajo que éste proceso representa, es sin duda el motivo principal y la razón de ser de la presente investigación.

Palabras Clave: Cifrado, Criptografía, ISO 27001, Raspberry, Seguridad de la Información.

ABSTRACT

With advances in information technology, more and more processes are automated, the centralization of information becomes a necessity, and the transport of information throughout the network must be done in a safe and fast way, it is necessary to use mechanisms that support this first factor, and one of them is cryptography.

There is more than one cryptographic mechanism that can be used to provide information security, using different platforms and software, but very little or nothing has been done on this type of research on platforms with single-board devices.

Due to the limited characteristics of single-chip microcomputers, it is necessary to carry out the present investigation, because as these devices are known as Raspberry, the low cost, easy maintenance, reduced size and great resistance to deterioration factors such as weather, humidity, dust, even insect attacks, are advantages offered by the use of this type of devices for agricultural companies.

Find an algorithm that provides the necessary security without causing a faint in the operation of the device caused by the workload that this process represents, is undoubtedly the main reason and rationale of the present investigation.

Keywords: Encryption, Cryptography, ISO 27001, Raspberry, Security of Information.

Introducción

En la informática, uno de puntos neurálgicos al momento de iniciar las actividades una empresa, es la seguridad, son varios los aspectos a considerarse al tratarse de este tema, y uno de ellos es la seguridad en la transmisión de datos desde los aplicativos hasta sus respectivos repositorios.

Son muchos los métodos de seguridad aplicables, uno de ellos es la encriptación de datos, existe mucha información en la red sobre las características, ventajas y desventajas de cada uno de los diferentes mecanismos de encriptación, implementados en equipos computacionales con características robustas y los resultados son muy satisfactorios.

Sin embargo, cuando estos mecanismos de cifrado se aplican en equipos limitados en cuanto a capacidad y velocidad de proceso los resultados son diferentes.

Es por ello que, en la presente investigación se realizarán pruebas de cifrado con 2 algoritmos, cada uno con estructuras diferentes, en equipos de Raspberry Pi2, donde se identificará entre otras variables: la respuesta de los equipos en cuanto a velocidad de cifrado y carga de trabajo.

Generalmente los dispositivos Raspberry se han utilizado para desarrollo a nivel didáctico por la facilidad de adquisición y mantenimiento, pero en la actualidad se está implementando este tipo de equipos en proyectos en empresas agrícolas precisamente por las características anteriormente mencionadas.

Situación Problemática

En la actualidad, el avance tecnológico está llegando a todas las áreas de todo tipo de negocio y la agricultura no ha sido la excepción. El Sistema de Balanzas Electrónicas (SBE) es un sistema informático web, mediante el cual se registran datos del proceso de embalaje de fruta en sus estaciones de trabajo, donde toda esta información es almacenada en equipos locales, durante las labores habituales, razón por la cual al terminar el proceso diario la información es recolectada en la aplicación cliente y migrado a un repositorio, donde es tabulada y procesada para su automatización por parte de los departamentos administrativos.

Puesto que el envío se realiza diariamente, mediante la intranet de la empresa, la cual también es utilizada para la transmisión de toda la información de cada sucursal, mismas que están ubicadas en varias provincias (Los Ríos, Santo Domingo, Guayas, Machala, Manabí y Bolívar), y que se genera diariamente el control de asistencia, materiales retirados y utilizados en bodega, alimentación del personal, labores de campo, entre otras. Es importante describir que son necesarios estos procesos para llevar el control de los productos terminados diariamente y poder cumplir con los respectivos cupos según cada marca y cliente, por lo que es muy importante que ésta llegue de una forma rápida y segura.

Actualmente los envíos de datos de producción se lo están realizando sin ningún tipo de seguridad en la transmisión, por lo que no resultaría difícil interceptarla y modificarla o sencillamente corromperla comprometiendo su integridad.

Ahora bien, pensando en lo mencionado en el párrafo anterior, la empresa necesitaría un mecanismo de cifrado que asegure la transmisión y recepción de la información, y que su contenido esté protegido, pero a la vez, sin provocar un colapso de la intranet, induciendo a los demás usuarios de la red al retraso en sus labores, por lo que es muy importante elegir el mecanismo de seguridad adecuado que mantenga el equilibrio perfecto entre seguridad y manejo de datos.

Problema Científico

En el siguiente punto surge la interrogante ¿Cuál sería un mecanismo de cifrado que se adapte tanto al medio de trabajo de las empresas en estudio, como a los recursos limitados en hardware que supone Raspberry, y que a la vez garantice un flujo uniforme sin que existan desmayos en los procesos y en la red?

Objeto de estudio

El principal objetivo de la presente investigación es diferenciar las particularidades de los diversos sistemas de encriptación y su rendimiento en plataformas, con características de hardware reducidas, llegando a alcanzar armonía entre carga de proceso y tiempos de respuesta.

En sí mismo cada mecanismo de cifrado posee un funcionamiento diferente al de los demás, lo que supone cargas de trabajo diferentes. Los dispositivos Raspberry aun en su versión más actual cuentan con características de procesamiento que limita sus funciones, por lo que es necesario realizar pruebas en sus ambientes más extremos para considerarlos idóneos antes de su lanzamiento a producción.

Campo de investigación

En la actualidad el campo de aplicación para dispositivos Raspberry se está ampliando, por su bajo costo, fácil mantenimiento y gran resistencia a ambientes hostiles. Con el acoplamiento correcto, como sensores de humedad, de movimiento, de temperatura, detectores de agentes químicos y muchas otras variantes este tipo de dispositivos se está utilizando cada vez con mayor frecuencia sobre todo en el área agrícola.

En las empresas agrícolas se las utiliza en el campo, en áreas donde no es posible tener instalaciones adecuadas para computadores de escritorio convencionales, donde se utilizan con aplicaciones dedicadas, acumulan información y la envían hasta repositorios ubicados en otras ciudades.

Como el resto de la información de las diferentes áreas, ésta información también es importante para la empresa, y debe ser tratada con cuidado, asegurando los pilares fundamentales de su seguridad como confidencialidad, integridad y disponibilidad.

Consecuentemente, lo que se espera con el presente proyecto es dejar disponible información acerca de resultados de ensayos realizados en campo sobre el comportamiento de estos dispositivos utilizando mecanismos de cifrado diferentes.

Objetivo General.

1. Analizar el rendimiento de tecnologías criptográficas, basado en la Norma ISO 27001 y 27002, durante la transferencia en la capa de Transporte con dispositivos Raspberry PI.

Objetivos Específicos.

1. Fundamentar un algoritmo de encriptación, para proteger la transmisión de datos de manera segura, utilizando estándares y políticas de seguridad de la información.
2. Examinar el rendimiento de procesos criptográficos que sean ligeros y efectivos, y que no comprometa el valor computacional de los dispositivos Raspberry con S.O. Debian.
3. Establecer un algoritmo de encriptación que garantice el correcto funcionamiento de las operaciones, fundamentado en el literal 8 de las ISO 27001 y en el control 10.1 de la sección 10 de la ISO 27002.

Justificación de la Investigación

A continuación, la presente investigación ayudará a decidir qué mecanismo de cifrado es el correcto para este tipo de entorno, el equilibrio entre la carga de trabajo y un nivel óptimo de cifrado debe ser el adecuado, sobre todo teniendo en cuenta los recursos limitados con que cuenta el Sistema de Balanzas Electrónicas (SBE).

En la actualidad existe una extensa diversidad de técnicas criptográficas, y saber elegir la herramienta adecuada exige un análisis exhaustivo de sus características conociendo su clasificación y conceptos fundamentales, para poder darle un uso adecuado y sacar el mayor beneficio posible.

Los dispositivos Raspberry cuentan con una memoria y un procesador reducidos, mientras que los algoritmos que serán analizados necesitan cierta capacidad para poder funcionar correctamente, es por eso que se estas pruebas darán indicadores que ayudara a tomar una decisión adecuada con respecto de que algoritmo es el más adecuado para este entorno de trabajo.

Resumiendo, la actual investigación dejara un antecedente sobre tecnologías que se adapten a ambientes agrícolas con recursos de hardware y software mínimos, y que ofrezcan resultados apropiados.

CAPÍTULO I

MARCO TEÓRICO

1.1. Antecedentes Investigativos

La información transmitida mediante redes de comunicaciones se encuentra expuesta a disímiles eventos inducidos por quienes buscan apropiarse de la misma. Por ello, Algaba et al, (2017) describen que *“la información se ha transformado en un activo esencial para las entidades y para su desarrollo organizativo”*. Por esta razón, las empresas han generado e integrado sistemas que la ayudan a incrementar sus beneficios, siendo necesario para ello herramientas que permitan resguardar los datos que transitan por la red.

Lo expuesto en el párrafo anterior, deja claro la importancia de la información en las empresas, teniendo en cuenta que existen muchos tipos de amenazas y riesgos a los que este recurso está expuesto, por lo cual, Jean-François (2016), expone un concepto claro sobre este tipo de situaciones: *“una amenaza es alguien o algo que puede explotar una vulnerabilidad para obtener, modificar o impedir el acceso a un activo o comprometerlo”*.

De aquí que la realización de la presente investigación es de vital importancia pues siendo la información con carácter confidencial, compromete la seguridad de las personas, organizaciones y/o gobiernos, los mismos que han sufrido varias amenazas relacionadas con la divulgación de información en los últimos años. Siendo esencial considerar e instaurar los parámetros de seguridad al implantar una red de comunicaciones.

En el país, el sector de las empresas agrícolas, y específicamente en las áreas que se encuentran físicamente en lugares apartados del casco urbano, normalmente no se cuenta con infraestructuras sólidas, modernas o que al menos cuenten con todo el poder computacional que se desea, así lo confirman (Ramirez Morales & Mazon Olivo, 2017), *“en Latinoamérica, cada día el uso de los datos agropecuarios para el desarrollo de aplicaciones informáticas se está extendiendo, no solo para el beneficio del agricultor que la genera, sino de toda una cadena de valor, que admite realizar una revisión segura de los registros”*.

Teniendo en cuenta que el principal elemento en esta investigación es la información, y el propósito de estudio es encontrar un mecanismo de cifrado que cubra lo necesario en la temática de la seguridad, ha sido necesario recurrir a compendios en diferentes temas para

alcanzar una síntesis que reúna las definiciones de cada tema que ayude aclarando la investigación realizada.

A continuación, se detalla uno a uno estos elementos:

1.2. Redes Inalámbricas

En la actualidad se ha visto un gran crecimiento en los dispositivos móviles, lo que a su vez ha hecho crecer también la necesidad de conexiones que no necesiten cableado físico, los tipos de esta forma de comunicación se identifican de la siguiente manera:

1.2.1. WAN

Es una red de área extensa, que puede abarcar países y hasta continentes, pero también este término es aplicable a una empresa que tiene una central y varias sucursales lo suficientemente distantes.

Entre sus principales características destacan:

- Pueden abarcar superficies muy amplias
- Tasa de transmisión de datos restringida
- Mayor probabilidad de interferencia

Debido a las largas distancias que pueden llegar a cubrir, pueden llegar a necesitar puentes o repetidores, lo que aumenta la probabilidad de llegar a sufrir interferencias.

Cuando la distancia es relativamente mayor, se puede llegar a tener que recurrir a empresas de telecomunicaciones como microondas, telefónicas o satelitales.

Un ejemplo apropiado para este tipo de red sería el internet, pues está interconectando millones de computadores a nivel mundial, que en su gran mayoría a la vez están formando grupos de computadores más pequeños llamadas redes LAN.

1.2.2. LAN

A diferencia de las redes WAN, las LAN se limitan a un edificio o edificios contiguos llegando a tener las siguientes características:

- Pueden abarcar extensiones con superficies limitadas
- Poseen tasas de transmisión de datos más altas en comparación con las redes WAN
- Mayor resistencia a las interferencias
- La capa de transporte (cable) es de uso privado

El mismo hecho de las cercanías entre los dispositivos, provoca que la tasa de transferencia de datos aumente y la probabilidad de interferencia disminuya.

1.2.3. WLAN

Caracterizada principalmente por prescindir de cableado, una WLAN comunica dispositivos electrónicos entre sí por medio de emisiones radioeléctricas propagadas en el aire. Pueden cubrir espacios no extensos, como oficinas, una casa, comedores públicos, bibliotecas, salas de espera, entre otras.

Las ventajas más significativas son:

- Movilidad a los usuarios
- Sencilla instalación y con costos bajos
- Itinerancia a usuarios con dispositivos móviles

Utilizada en gran parte como alternativa a la LAN y en otros casos como extensión a esta, en lugares donde por infraestructura o determinada condición lo requiere.

1.3. Dispositivos Electrónicos

Entre los dispositivos que se utilizarán para realizar las pruebas de la investigación se tiene, entre otros:

- Microordenador de tarjeta integrada
- Dispositivos Wireless
- Tecnología WSN

1.3.1. Raspberry PI

De acuerdo con González (2014), Raspberry es un microcomputador de placa simple de bajo coste, desarrollado inicialmente con fines educativos. Aunque su SO de código abierto oficial es una versión adaptada de Debian a la que se denominó Raspbian, también permite otros sistemas operativos como Windows 10 en su versión adaptada.

Raspberry Pi es un dispositivo que requiere accesorios, los cuales son comprados por separado según el proyecto que se desee realizar; algunos de los accesorios que se pueden utilizar son una tarjeta SD, un teclado, un Mouse, un mini adaptador externo USB y un cable HDMI o de video compuesto RCA.

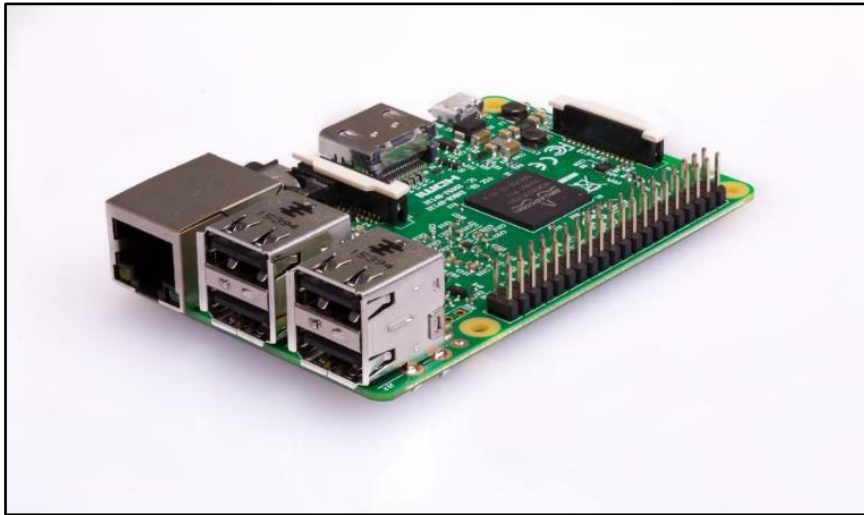


Figura 1. Raspberry Pi3, Cara superior
Fuente: www.raspberrypi.org

En la figura N° 1 se presenta la imagen de la cara superior de la Raspberry PI 3, con sus conectores para periféricos, pines configurables, procesadores y de red, todo montado en su placa única.

Actualmente el último producto lanzado por la Fundación Raspberry PI es la Raspberry Pi 3 Modelo B +, que presenta las características de hardware siguientes:

- Quad Core 1.2GHz Broadcom BCM2837 64bit CPU
- 1 GB de RAM
- BCM43438 LAN inalámbrica y Bluetooth Low Energy (BLE)

- 100 Base Ethernet
- GPIO extendido de 40 pines
- 4 puertos USB 2
- Salida de 4 polos estéreo y puerto de video compuesto
- HDMI de tamaño completo
- Puerto de cámara CSI para conectar una cámara Raspberry Pi
- Puerto de pantalla DSI para conectar una pantalla táctil Raspberry Pi
- Puerto micro SD para cargar su sistema operativo y almacenar datos
- Fuente de alimentación Micro USB conmutada actualizada de hasta 2.5A

En el presente proyecto se utilizará dispositivos Raspberry PI 3, como hardware para las pruebas donde se medirá la respuesta en cuanto a velocidad de proceso al aplicar algoritmos de cifrado 3DES y RSA.

1.3.2. Arduino

La empresa Software in the Public Interest Inc, especifica en su portal que, Arduino es una plataforma de prototipo electrónica de código abierto que se comunica a través de disímiles sensores que controlan elementos del entorno. Los proyectos que utilizan placas Arduino pueden funcionar de forma independientes o comunicarse vía software a una pc, el microcontrolador se programa usando el “Lenguaje de Programación Arduino” y Entorno de desarrollo Arduino”. (Software in the Public Interest, Inc, 2018)

Ahora bien, Arduino inicio como una herramienta didáctica para quienes estaban iniciando su carrera como estudiantes de electrónica y programación, pero con el tiempo se extendió adaptándose a nuevos cambios y desafíos.

Al ser completamente de código abierto, permite que el usuario adapte al dispositivo a su entorno particular, además de aumentar su crecimiento exponencialmente gracias a los aportes de las comunidades que la utilizan.

Las ventajas que destacan de Arduino se las enumera a continuación:

- **Bajo costo:** Las placas Arduino son más económicas comparativamente con otros tableros de microcontroladores. La versión de menos costo puede ser acoplada a mano.
- **Multiplataforma:** El software de Arduino (IDE) corre sobre varios sistemas operativos entre ellos: Windows, Macintosh OS X, y Linux. Sin embargo, los otros tipos de microcontroladores la mayoría solo se ejecutan sobre Windows.
- **IDE sencillo y claro:** El software es fácil de usar para quienes comienzan a utilizarlo por primera vez y al mismo tiempo extremadamente flexible siendo aprovechado por usuarios avanzados. De igual forma al estar enfocado en el entorno de programación “Processing” los estudiantes familiarizados con este entorno aprenden rápidamente el funcionamiento del IDE.
- **Software de código abierto y extensible:** Se publica como código abierto y expandible por programadores experimentados mediante bibliotecas de C ++.
- **Fuente abierta y hardware extensible:** Los diseñadores de circuitos más experimentados pueden desarrollar su propia versión de los planes de tableros, ampliarlos o mejorarlos al estar publicados bajo licencia “Creative Commons”.

La Tabla 1 recoge los tipos de placas más importantes del mercado con sus características:

Tabla 1. Especificaciones técnicas de placas Arduino.

Descripción	Procesador	Operación / voltaje de entrada	Velocidad de la CPU	Analógica In / Out	IO / PWM digital	EEPROM [kB]	SRAM [kB]	Flash [kB]	USB	UART
101	Intel® Curie	3.3 V / 7-12V	32MHz	6/0	14/4	-	24	196	Regular	-
Gema	ATtiny85	3.3 V / 4-16 V	8 MHz	1/0	3/2	0.5	0.5	8	Micro	0
LilyPad SimpleSnap	ATmega328P	2.7-5.5 V	8 MHz	4/0	9/4	1	2	32	-	-
LilyPad USB	ATmega32U4	3.3 V / 3.8-5 V	8 MHz	4/0	9/4	1	2.5	32	Micro	-
Mega 2560	ATmega2560	5 V / 7-12 V	16 MHz	16/0	54/15	4	8	256	Regular	4
Micro	ATmega32U4	5 V / 7-12 V	16 MHz	12/0	20/7	1	2.5	32	Micro	1
MKR1000	SAMD21 Cortex-M0 +	3.3 V / 5V	48MHz	7/1	8/4	-	32	256	Micro	1

Pro	ATmega168	3.3 V / 3.35-12 V	8 MHz	6/0	14/6	0.512	1	16	-	1
Pro Mini	ATmega328P	3.3 V / 3.35-12 V	8 MHz	6/0	14/6	1	2	32	-	1
Cero	ATSAMD21 G18	3.3 V / 7-12 V	48 MHz	6/1	14/10	-	32	256	2 micro	2
Debido	ATSAM3X8 E	3.3 V / 7-12 V	84 MHz	7/1	54/12	-	96	512	2 micro	4
Esplora	ATmega32U4	5 V / 7-12 V	16 MHz	-	-	1	2.5	32	Micro	-
Ethernet	ATmega328P	5 V / 7-12 V	16 MHz	6/0	14/4	1	2	32	Regular	-
Leonardo	ATmega32U4	5 V / 7-12 V	16 MHz	12/0	20/7	1	2.5	32	Micro	1
Mega ADK	ATmega2560	5 V / 7-12 V	16 MHz	16/0	54/15	4	8	256	Regular	4
Uno	ATmega328P	5 V / 7-12 V	16 MHz	6/0	14/6	1	2	32	Regular	1

Esta tabla muestra una lista de las especificaciones técnicas de las características de todas las placas Arduino genuinas.

1.3.3. Conexión Wireless

WiFi/802.11 es considerado un estándar en cuanto a redes inalámbricas, además, manifiesta Rossiñol (2015), que IEEE 802 fuera desarrollado para redes locales inalámbricas, ofreciendo gran flexibilidad a los usuarios por su fácil conexión y su itinerancia con dispositivos móviles.

Existen diversas tipologías de wifi, basados todos en un estándar IEEE 802.11 y son los presentados a continuación:

- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

Todas estas variantes están reconocidas en el ámbito mundial a partir de la generalización en el uso de la banda 2,4 GHz que tienen velocidades de 11Mbit/s, 54 Mbit/s y 300 Mbit/s, respectivamente.

Actualmente también se maneja el estándar IEEE 802.11ac, o también conocido como WIFI 5, que trabaja en la banda de 5 GHz recién habilitada con canales que tienen pocas interferencias al no existir tecnologías como Bluetooth, microondas que puedan interferir en la comunicación. Sin embargo, al tener una frecuencia mayor que los estándares que usan banda 2,4 GHz estos poseen un alcance mucho menor que puede ser de hasta un 10%

1.4. Sistemas Operativos de código abierto

1.4.1. Linux

Basado en el Sistema Operativo (SO) Unix, multitarea y multiusuario, Linux fue desarrollado por Linus Benedict Torvalds en 1991, para su uso en computadores personales, destaca sobre Unix por ser de código abierto y de libre distribución. Dicho SO, ha avanzado mucho en los últimos años, no solo en sus mejoras de interfaces gráficas de usuario, sino también en la mejora en cuanto al aprovechamiento del hardware, lo que lo ha hecho más eficiente.

Por lo dicho, Goñi (2015) indica que al publicar Torvalds su código, su sistema operativo tuvo la acogida de muchas personas interesadas, Richard Stallman fundador de Fundación de Software Libre era uno de ellos (Goñi, 2005). Stallman quería crear un sistema operativo con sus propios programas y poner a disposición del público en general el código fuente, fue entonces que se unieron Torvalds, Stallman y quienes desarrollaban para GNU, fue entonces que nació GNU/Linux.

1.4.2. Debian

De acuerdo con la empresa Software in the Public Interest Inc, los sistemas operativos desarrollos computacionales que permite al usuario comunicarse con la computadora. Los sistemas operativos poseen un núcleo que efectúa todas las operaciones básicas y al mismo tiempo brinda la posibilidad de ejecución de otros programas; por lo que constituye el modulo más importante del funcionamiento del sistema operativo. La mayoría de las utilidades básicas que completan el sistema como: GNU/Linux, GNU/kFreeBSD, y GNU/Hurd, provienen del proyecto GNU por lo que también son de uso libre. (Software in the Public Interest, Inc, 2018)

En los dispositivos Raspberry PI3 se utilizan NOOBS (New Out of Box Software), y se descarga la versión Debian para Raspberry, también llamada Raspbian, este Sistema Operativo servirá de plataforma para la aplicación web SBE, y será donde se ejecutará los algoritmos de encriptación que servirán para someter a prueba el hardware.

1.5. Software Analizador de Protocolos

Un analizador de protocolos es una herramienta que sirve para depurar y desarrollar protocolos, además de aplicaciones basadas en red. Además, es considerada como una herramienta didáctica de gran ayuda para analizar tramas que son capturadas en su paso por la capa de transporte, ayudando al equipo de desarrolladores de protocolos a encontrar posibles deficiencias de red en concreto, ahorrando al analista tener que desplazarse largas distancias.

Entre los analizadores más conocidos se tiene los siguientes:

- Wireshark
- Nagios
- Netflow

1.5.1. Wireshark

Es un analizador de protocolos muy utilizado para realizar análisis a redes de comunicación, además de su uso para el desarrollo de software y de protocolos y una potente herramienta pedagógica. Accede a la información que transita en a través de la red, permitiendo encontrar fallas o errores en los datos.

Desarrollado bajo software libre y mantenido bajo licencia GPL, es compatible con la mayoría de sistemas operativos conocidos, tiene más de 480 protocolos y permite el análisis de sumarios a través de paquetes capturados.

Algo importante de destacar de Wireshark es que es un analizador de protocolos pasivo, es decir, no manipula los datos, solo los inspecciona en busca de comportamientos extraños en los datos analizados, ayudando a encontrar problemas de red si los hubiera.

Rossiñol (2015), manifiesta que es probable que debido a falta de documentación se presenten situaciones en las que Wireshark no sea capaz de interpretar ciertos protocolos, donde la mejor manera de afrontar la situación sea la ingeniería inversa.

En este proyecto, Wireshark ayudará a interceptar la información que se transfieran desde las estaciones de trabajo hasta el repositorio central, y se podrá ver si es posible conocer el contenido de los archivos.

1.5.2. Nagios

Ampliamente utilizado, Nagios es un software creado para la monitorización de servicios de red, siendo de software libre, fue diseñado originalmente para su ejecución bajo GNU/Linux, tiene como característica principal la vigilancia de equipos y software que estén definidos, dando alertas en el caso de descubrir comportamientos fuera de lo normal.

Llamado inicialmente NetSaint, debió cambiársele el nombre por parecidos con nombres de otras marcas comerciales, en la práctica Granados (2006), explica que Nagios realiza la gestión de red mediante su interfaz web, con una amplia gama de parámetros y en distintos protocolos como por ejemplo SNMP.

Una característica destacable de Nagios es su potente sistema de plugins, como son: independencia de plataforma, múltiples vías de notificaciones, monitoreo remoto mediante

SSL/SSH, gráficos de informes de rendimiento, definición de manejadores de eventos y fácil escalabilidad.

1.5.3. Netflow

Desarrollado por Cisco Systems Inc, Netflow recolecta información sobre tráfico IP, convirtiéndose en un estándar en la industria de la monitorización de tráfico de red. Soportada en Linux, FreeBSD, NetBSD, además de varias plataformas de fabricantes de dispositivos como: Cisco IOS, Juniper, Enterasys Switches entre otras.

Es importante conocer que Cisco IOS Nerflow proporciona servicios para aplicaciones IP como: contabilidad de tráfico de red, facturación de red basada en uso, seguridades, administración de negación de servicios y constante supervisión de red.

De acuerdo con la última publicación en su portal web Muñoz (2017), señala que NetFlow es una herramienta integrada dentro del software Cisco IOS para identificar el funcionamiento de la red, sobre todo considerando que la visibilidad en la red es una herramienta indispensable para los profesionales de TI. Por lo que es indispensable conocer cuál es el comportamiento que esta presentado la red, además de:

- Aplicación y uso de la red.
- Productividad de la red y utilización de los recursos de la red.
- El impacto de los cambios en la red.
- Anomalías de red y vulnerabilidades de seguridad.
- Problemas de cumplimiento a largo plazo

Cisco IOS NetFlow precisamente, satisface esas necesidades, creando un entorno donde los administradores tienen las herramientas para entender quién, qué, cuándo, dónde y cómo fluye el tráfico de la red. Cuando se conoce el comportamiento de la red, el proceso de negocios mejora y estará disponible un registro de auditoría de cómo se está utilizando la red.

Esta mayor conciencia reduce la vulnerabilidad de la red en relación con la interrupción del servicio y permite un funcionamiento eficiente, mejorando las operaciones de la red,

reduciendo los costos e incrementando los ingresos del negocio al utilizar mejor la infraestructura de la red.

1.6. Arquitectura SBC (Computadores de Placa Reducida)

Sobre estas arquitecturas Caballero & Clavero (2017), comenta que, hoy en día la tendencia en cuanto al desarrollo tecnológico está basada en mejorar la relación costo-beneficio de los dispositivos desarrollados, es por ello necesario incursionar en nuevos campos como lo son los computadores de placa reducida; con dimensiones pequeñas, pero con características muy similares a las de un computador funcional, excepto por una gran diferencia: de costo.

Ahora bien, Caballero & Clavero (2017), manifiesta que, un ordenador de placa reducida (en inglés: Single Board Computer o SBC) es un computador completo en un sólo circuito, basando su diseño en un sólo microprocesador, con todos los componentes y características de un computador convencional y en una sola placa, que suele ser de tamaño mínimo, y que tiene todo lo necesario integrado en la tarjeta.

1.6.1. Aplicaciones

A pesar de que la tendencia de los últimos años indica que puede haber cambios, estos dispositivos aún no se usan como computadores personales, sino más bien en entornos industriales o inmersos como parte de otros sistemas más grandes.

Gracias a su completa integración, estos dispositivos reducen enormemente su tamaño, su peso y su consumo de energía, y algo muy importante, su costo, lo que lo hace una buena opción para entornos con infraestructura deficientes.

Por otro lado, tanto la actualización del hardware como su mantenimiento se vuelve relativamente insostenible, por lo que, en cualquier caso, lo que se espera es el reemplazo del componente entero.

Entre las principales o más comunes aplicaciones que se dan a este tipo de arquitectura se tiene:

- Industria
- Domótica

- Entornos de alta seguridad.
- Medio ambiente
- Medicina

1.6.2. Redes WSN (Industria)

Siguiendo con Ariansen & Rojas (2017), con respecto de las Redes Inalámbricas de Sensores, se conoce que los últimos avances tecnológicos que mantienen estrecha relación con las TIC, permiten obtener información por diferentes medios de comunicación, entornos de difícil acceso, costos de instalación bajos y se debe de mantener vínculos de conexión fijos permanentemente.

Entre sus principales propiedades se pueden destacar:

Ventajas

- No requieren de asistencia física permanente
- Adaptabilidad a climas extremos
- Autoconfiguración de nodos
- Autonomía para la generación de información de los nodos
- Bajo costo de hardware
- Gran tamaño de la red, sin perder robustez
- Fácil implementación.

Desventajas

- Tiempo de uso limitado
- Recurso energético limitado
- Dependencia del Gateway o nodo central, al fallar este, todos sus nodos dejan de transmitir

a. Aplicaciones

Entre los usos más comunes para las tecnologías WSN se encuentran las siguientes:

- Agricultura de precisión
- Supervisión del medio ambiente (Sismología)
- Detección acústica
- Control en actividades nucleares
- Aplicaciones militares
- Gestión de tráfico vehicular
- Entre otros.

1.6.2.1. Agricultura de precisión.

Son técnicas de optimización de recursos naturales que permiten gestionar sobre la base de la observación, medición y actuación, aplicaciones agrícolas como riego, control de temperaturas, estados de los suelos, entre otras muchas aplicaciones específicas. Los datos recolectados pueden ser utilizados en la evaluación y estimación de la densidad óptima de siembra y cantidad adecuada de fertilizantes o de otros insumos necesarios. Además, permiten predecir con más exactitud el rendimiento y la producción de los cultivos.

Guaña (2016), describe que la agricultura de precisión ha cambiado los paradigmas convencionales, ya que los beneficios que ofrecen beneficios potenciales de rentabilidad, productividad, sostenibilidad, calidad de los cultivos, protección de los suelos, seguridad alimentaria y desarrollo económico rural de los pueblos.

Pensando en aumentar la eficiencia y la eficacia del uso de los diferentes recursos agrícolas, la agricultura de precisión se ha enfocado en aplicaciones innovadoras, permitiendo integrar y estandarizar el nivel de calidad de la gestión de los sembríos.

Entre las técnicas que intervienen en un proceso de Agricultura de precisión se tiene:

a. **Recopilación de la información.**

Generación de registros de actividades que permiten obtener una estadística de la situación real en la que se encuentra el cultivo, que es almacenada en repositorios centrales para su posterior análisis.

b. **Procesamiento de la información recolectada.**

Esta información es analizada y utilizada para la posterior toma de decisión en cuanto a los procesos en las labores agrícolas.

c. **Aplicación del conocimiento.**

Los procesos de gestión mejorarán, se aprovecharán mejor los recursos, aplicando solo lo necesario en cuanto a productos químicos y demás, evitando dañar al cultivo y al medio ambiente en general.

1.6.3. Domótica

La domótica es el conjunto de técnicas o metodologías que se utilizan para llevar a cabo la automatización de una vivienda o edificación de cualquier tipo, colaborando con el mejoramiento, gestión o servicio con relación a la seguridad, energía, bienestar o comunicación.

La interconexión puede ser por medio de cables o inalámbrica y su monitoreo puede ser localmente o desde otro lugar mediante la internet.

a. **Arquitectura**

Según de cómo se encuentra la inteligencia en un sistema domótico, podemos describir varios tipos de arquitecturas:

- **Arquitectura centralizada:** Se denomina arquitectura centralizada cuando un controlador centralizado recibe toda la información de variados sensores, la procesa y genera las ordenanzas pertinentes para los actuadores.

- **Arquitectura distribuida:** Es cuando la inteligencia del sistema se encuentra distribuida entre los diferentes. Frecuentemente lo encontramos en los sistemas cableados en bus, o en redes inalámbricas.
- **Arquitectura mixta:** Poseen una descentralizada, pues tienen varios dispositivos menores capaces de obtener y analizar la información de varios sensores y retransmitirlos a los demás dispositivos distribuidos por toda la vivienda.

1.7. Seguridad de la Información

Por ser la información un recurso tan importante en toda empresa, es significativo entender su definición, según Rossiñol (2015), la información permite gestionar, formalizar y condicionar el conocimiento nuevo. De aquí que la información tenga un sentido pragmático, pues se materializa en informes investigativos, noticias u otras formas de transmisión de conocimiento. Dejando de esta manera distinguir que esta generación y comunicación de la información forma parte vital de cualquier empresa.

Además, según Tanenbaum (2003), son una serie de actividades que proveen que el sistema mantenga su disponibilidad, posibilidades de procesamiento, espacio de almacenamiento y mantenga de forma íntegra la información del mismo.

Ahora bien, por el valor que se le da a este recurso, es no menos importante, la seguridad con que se la debe tratar. De acuerdo con López et al (2012), la Seguridad de la Información garantiza que todos o la mayoría de los riesgos de la seguridad sean conocidos, asumidos, gestionados y minimizados mediante una documentación sistemática, estructurada, eficiente y que pueda ser adaptada a los cambios producidos en los riesgos, el entorno y las tecnologías.

1.8. Algoritmos de Cifrado

Continuando con Granados (2006), la llegada y desarrollo de Internet y uso masivo de la computadora, se hace necesario la utilización de herramientas automatizadas que permiten la protección de documentos e información almacenada en las mismas. Algunas de estas utilidades son: los cortafuegos, los Sistemas Detectores de Intrusos y el uso de sistemas criptográficos; las mismas que permiten proteger tanto la información como a los Sistemas Informáticos encargados de administrarla.

1.8.1. 3DES

Este algoritmo descendiente del algoritmo DES, diseñado por IBM y publicado en 1975, inicialmente estandarizado para instituciones financieras, es actualmente uno de los algoritmos más utilizados por las tarjetas de crédito y otros medios de pago electrónico, no obstante, está desapareciendo lentamente debido a su proceso de cifrado que tiende a ser relativamente lento, y está siendo sustituido por el algoritmo AES, del cual a la fecha no se ha descubierto vulnerabilidades.

Según las normas ISO 27000, este algoritmo se basa en doblar la longitud efectiva de la clave a 112 bits, pero debido a la necesidad de triplicar el número de operaciones necesarias la longitud total de la clave será de 168 bits, sin modificar el algoritmo DES. (iso, 2018)

a. Funcionamiento de 3DES

La figura N° 2 presenta gráficamente cómo funciona el algoritmo 3DES con respecto a la gestión de su llave pública, y el proceso de cifrado y descifrado.

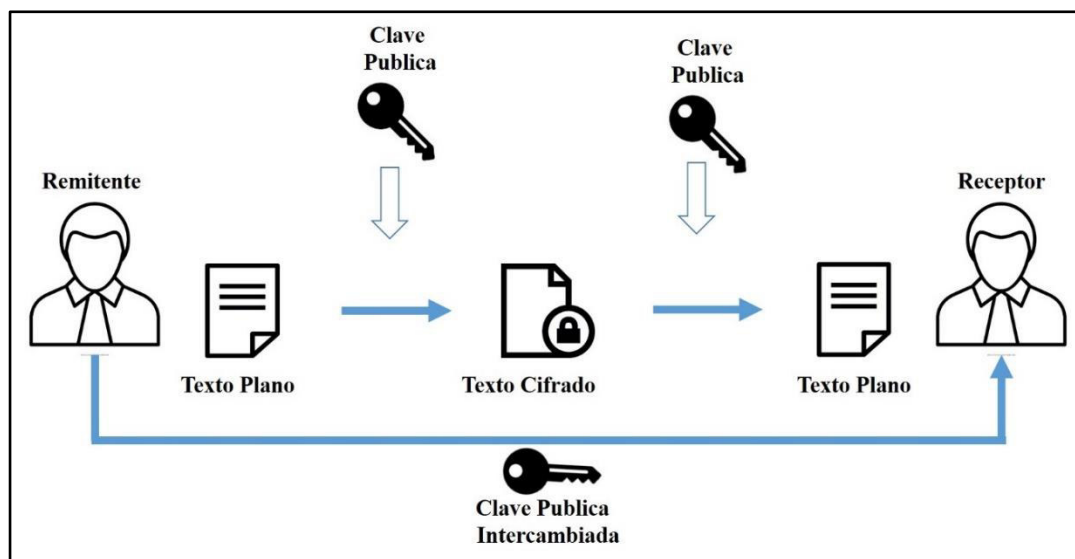


Figura 2. Modelo de funcionamiento del cifrado Simétrico.

Por otro lado, Cazu (2006) explica que el modelo de cifrado 3DES se basa en un algoritmo denominado 3DES-Encrypt-Decrypt-Encrypt que permite cifrar texto plano. Inicialmente se cifra el mensaje con una clave de 56 bits, luego en un segundo momento estos se descifran a través de claves de 56 bits y en un tercer momento la información es cifrada nuevamente utilizando una tercera clave de 56 bits.

En el siguiente gráfico se muestra la figura N° 3 y esta vez se presenta el funcionamiento del algoritmo 3DES con respecto al proceso de triple cifrado, tanto para cifrar el documento como para descifrarlo.

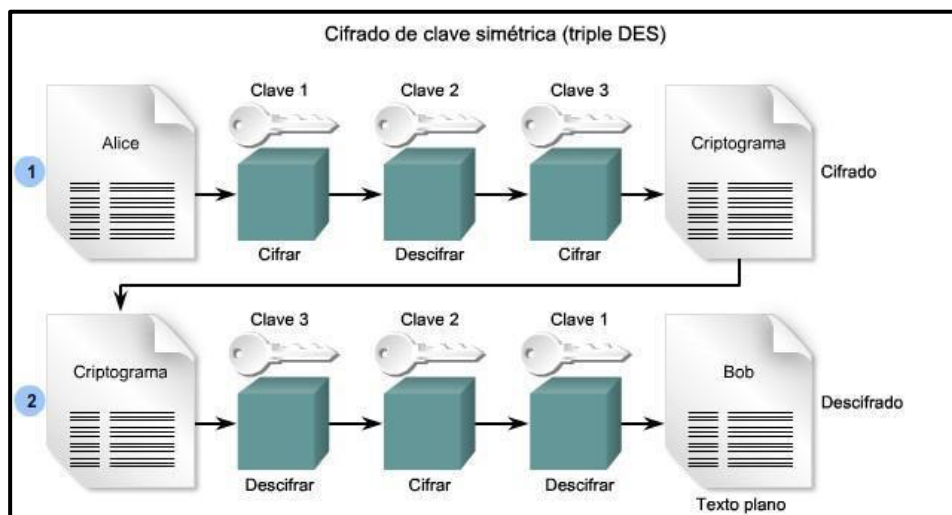


Figura 3. Funcionamiento del algoritmo de cifrado Triple Des
Fuente: (Ariansen & Rojas, 2017)

1.8.2. Rivest, Shamir y Adleman (RSA)

De acuerdo con Ander (1995), RSA es conocido por las iniciales de sus 3 descubridores (Rivest, Shamir y Adleman) y se estipula que este algoritmo se ha resistido a todos los intentos por romperlos por más de un cuarto de siglo, se le considera muy robusto. Su mayor desventaja es que requiere de claves de al menos 1024 bits para garantizar mayor seguridad, en comparación con 128 bits de los algoritmos de clave simétrica, lo que lo vuelve relativamente lento.

a. Algoritmo RSA

El algoritmo RSA consta de tres pasos básicos: Generación de claves, cifrado y descifrado.

Un breve ejemplo y explicación de su funcionamiento sería en siguiente:

- Si Oscar desea comunicarse con su amigo Byron de manera que solo Byron pueda leer el mensaje, debería:
- Oscar: Solicita a Byron una “caja de seguridad” abierta, la cual se maneja con dos llaves, una para cerrarla y otra para abrirla.

- Byron: Envía la caja abierta con la llave para cerrarla, la llave para abrirla se queda con Byron.
- Oscar: Escribe el mensaje y lo guarda dentro de la caja.
- Oscar: Cierra la caja con la llave de cerrar, en este punto, Oscar ya no puede ver el mensaje.
- Oscar: Envía la caja cerrada a Byron.
- Byron: Recibe la caja cerrada, usa su llave para abrir la caja y lee el mensaje.
- La llave para cerrar representa la clave pública de Byron, y la llave para abrir representa la clave privada.

La figura N° 4 presenta gráficamente cómo funciona el algoritmo RSA con respecto a la gestión de su clave pública y su clave privada, y el proceso de cifrado y descifrado.

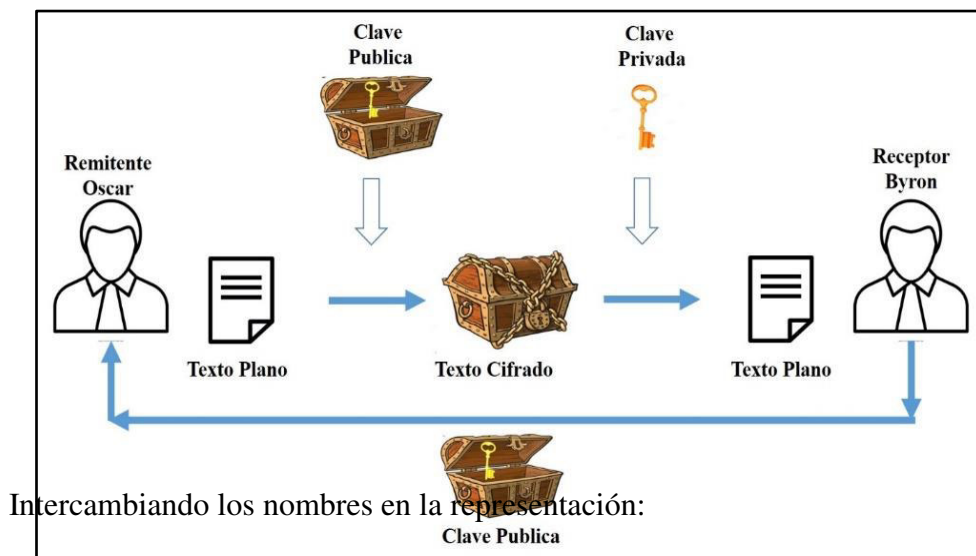


Figura 4. Modelo de funcionamiento del algoritmo asimétrico.

Texto Plano = M en forma de número m , menor que otro número n . Esto mediante un protocolo que puede ser reversado, conocido como “Patrón de relleno”.

El siguiente paso es el cifrado, c .

$$c \equiv m^e \pmod{n}$$

Donde e es la clave pública de Byron

Luego, para descifrar el mensaje c se utiliza la misma operación anterior a la inversa.

$$m \equiv c^d \pmod{n}$$

Donde d es la clave privada que solo Byron conoce.

Generación de claves. Para iniciar se debe escoger dos números primos aleatorios de igual longitud, diferentes entre sí: p y q

Luego se calcula n ,

$$n = p * q$$

Se calcula z , denominada Phi,

$$z(n) = [(p - 1) * (q - 1)]$$

Se obtiene un número k , éste es co-primo a z , z no es divisible por k .

La clave pública está lista, el conjunto de números (n, k) .

Para la clave privada se elige un número que cumpla:

$$k * j = 1 \pmod{z}$$

Luego, j sería la clave privada.

Cifrado del mensaje.

Se va a cifrar el texto plano P con la siguiente ecuación:

$$P^k = E \pmod{n}$$

Donde:

P es el mensaje sin cifrar

n y k son la clave pública

E es el mensaje cifrado

Descifrado del mensaje.

Una vez obtenido el mensaje cifrado E se procede a descifrarlo con la llave privada j que permanece en poder del destinatario realizando la siguiente operación:

$$E^j = P \pmod{n}$$

Donde:

E es el mensaje cifrado

j la llave privada

P es el mensaje sin cifrar

n es parte de la llave pública

1.9. Normas y Estándares

Compuesta por múltiples organizaciones internacionales de estandarización, es una organización para esquemas internacionales que promueve el uso de estándares propietarios, industriales y comerciales a nivel mundial.

Con sede en Ginebra, fue creada el 23 de febrero de 1947, y hasta el año 2015 se encontraba vigente en 196 países como una organización independiente no-gubernamental.

El uso de sus estándares hace que la creación de productos sea más seguros y confiables y de mejor calidad, logrando minimizar los gastos de producción y eliminando los errores, aumentando así la productividad y ganancias en los negocios a nivel mundial.

1.9.1. Normas ISO

Cema (2014), Definen las ISO/IEC 27000 como una serie de buenas prácticas establecidas por la “Organización Internacional de Estandarización” y la “Comisión Electrotécnica Internacional” que facilitan a las entidades gestionar la seguridad de la información (Cema,2014).

Esta serie de normas contienen buenas prácticas que permiten el diseño, desarrollo e implementación de los “Sistemas de Gestión de la Seguridad de la Información (SGSI)” y contiene otras normas que sirven de apoyo a la norma principal ISO/IEC 27001.

1.9.2. ISO / IEC 27001

Una publicación realizada por (Commons, Licencia Creative, 2018) describe el resumen de la relación de requisitos específicos de las cláusulas del estándar ISO/IEC 27001:2005 con los estándares que sirven de ayuda y/o desarrollo de posibles soluciones de implantación.

La figura N° 5 describe la relación entre la ISO/IEC: 27001 y las demás ISO de la misma familia que se extienden como anexos; relaciones que han cambiado debido a la publicación de la nueva versión de la norma ISO/IEC 27001:2013.

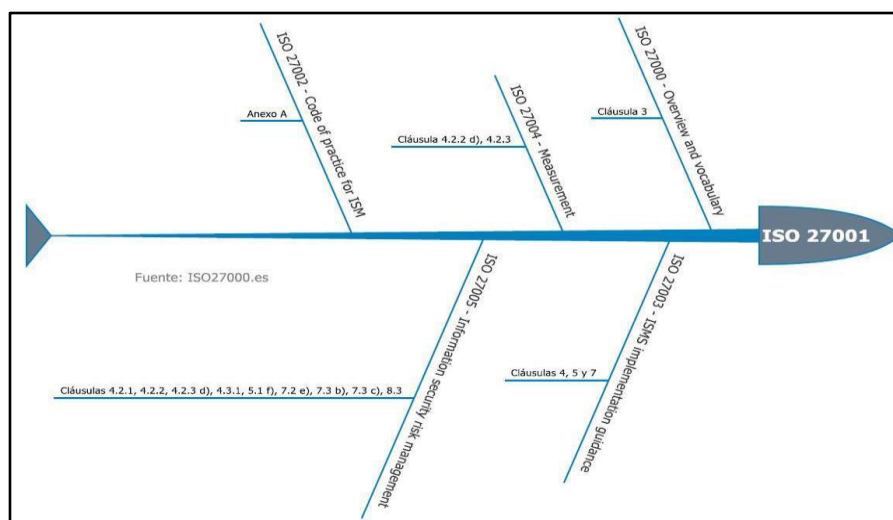


Figura 5. Relaciones Estándar ISO 27001 con otras ISO de la misma familia.

Fuente: (iso, 2018)

Finalmente la ISO 27001, que publicada en el año 2005 y actualizada nuevamente en el año 2013, constituye el documento principal que tiene todos los requisitos que debe tener un SGSI. (iso, 2018)

En la figura N° 5 de la norma ISO, especifican de forma resumida los objetivos y controles que se describen en la ISO/IEC 27002:2005, para ser seleccionados por las organizaciones en el desarrollo de sus SGSI. Debemos resaltar que, aunque no es obligatorio implementar todos los controles, las organizaciones que quieran implantar estas buenas prácticas deberán argumentar de forma sólida la no aplicabilidad de los controles no implementados.

Según la revista USERS, esta norma ayuda a proteger los activos de información otorgando confianza a todas las partes interesadas, esencialmente a los clientes. La misma adopta un enfoque por procesos que permite diseñar, implantar, implantar, monitorear y mejorar un SGSI, lo cual constituye una buena práctica adecuada para cualquier organización. (USERSHOP, 2015)

1.9.3. ISO / IEC 27002

Sobre la ISO 27002, describe que se publicó el 1 de julio de 2007, como una actualización de la ISO/IEC 17799:2005. Esta norma describe una guía para las políticas de seguridad de la información basada en 133 controles que se agrupan por once dominios de los procesos de la empresa. (iso, 2018)

CAPÍTULO II

MARCO METODOLOGICO

2.1. Metodología Investigativa

2.1.1. Investigación Descriptiva

De acuerdo con Cazau (2006), el presente estudio es descriptivo pues los conceptos seleccionados se miden de forma independiente, con el fin, de describirlas especificando las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno.

Además, se encontró que la investigación, es un proceso controlado conformado por varias fases o pasos que están conectados unos con otros de una manera lógica y secuencial que verifica permanentemente una comprobación y contrastación empírica de los hechos, fenómenos o procesos que se pretenden estudiar (Alegre Ramos, 2010).

Siguiendo estos conceptos, se puede indicar que las cuestiones en esta investigación son: ¿Qué mecanismo de cifrado es el que más se ajusta a los requerimientos y recursos?, ¿El nivel de seguridad es el adecuado?

También se describirán las variables, los tiempos de respuesta, tamaño de archivos. Se espera, luego de las pruebas contar con una base de conocimientos, que ayude a tomar las decisiones correctas, y que sirva de ayuda también para otras empresas que están incursionando en el área.

Por lo anterior expuesto, se ha definido el tipo de investigación como descriptiva, debido a que el análisis que se dará, está enfocado a evaluar variables en entornos independientes para resaltar las características favorables y desfavorables de cada una, en cada uno de sus procesos.

2.1.2. Diseño Experimental

Sobre el diseño experimental Jiménez (2015), dice que, este diseño estudia la forma en la que variables entran a ser parte de un proceso y producen un resultado a través de la interacción de las mismas.

El actual proyecto de investigación se ajusta a las características del diseño experimental, pretendiendo culminar con datos reales, demostrando de manera explicativa la relación causa-efecto.

Cumple, además, la investigación con los siguientes comportamientos en cuanto a enfoque y método de estudio:

2.1.3. Enfoque Cuantitativa

Debido a que se van a medir variables que determinarán al final de la investigación y rasgos importantes de cada uno de los algoritmos en sus respectivos escenarios, sacando a la luz sus debilidades y fortalezas en lo que respecta a variables como asignación de seguridad, velocidad de procesamiento, costo de carga, entre otros factores que serán medidos en equipos con recursos muy limitados.

2.2. Población y muestra

Para comprender mejor la estructura de la empresa en la que se desarrollara la investigación, a continuación, se presenta un diagrama en el que se detalla su organización a nivel de establecimientos.

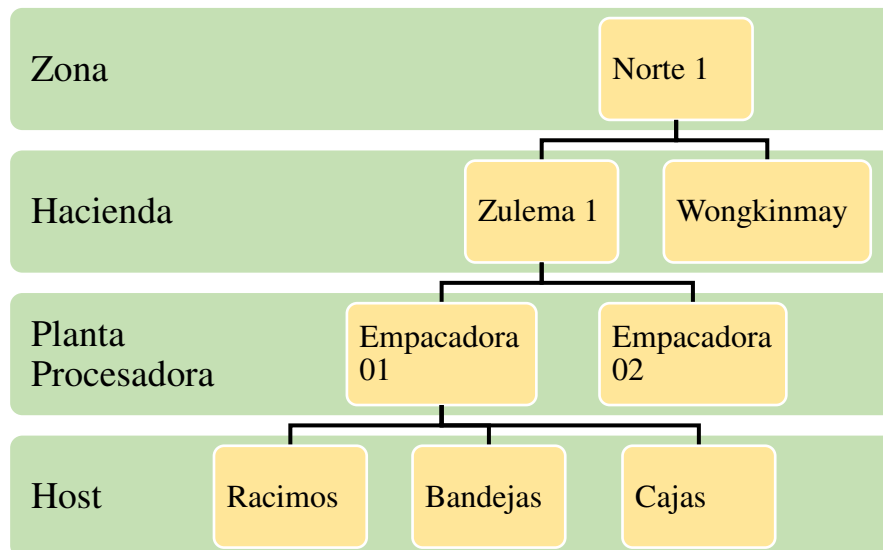


Figura 6. Organización estructural de los establecimientos

La figura N° 6 muestra cómo está establecida cada zona, pues cada una abarca entre 2 y 8 haciendas cercanas, existen 6 zonas en la organización. Una hacienda abarca entre 1 y 5 plantas procesadoras, existen 28 haciendas en total. Una Planta procesadora, también llamada empacadora, contiene 3 host o microcomputadores, existen 249 host en total en 83 empacadoras.

Tabla 2. Población de host

Fuente: Autor

Zona	Haciendas/Zona	Total Plantas Procesadoras	Total Host/Zona
Zona Norte 1	8	13	39
Zona Norte 2	4	16	48
Zona Centro 1	6	22	66
Zona Centro 2	4	19	57
Zona Sur 1	2	9	27
Zona Sur 2	4	4	12
Total Host:			249

En las 83 plantas procesadoras se encuentran 3 host en cada una.

2.2.1. Población.

La población en dicho proyecto de investigación será tomada en una empresa agrícola, donde cuentan con 83 plantas procesadoras con equipos Raspberry PI, los cuales están en producción de proceso de embalaje de fruta, y en cada planta de proceso están 3 estaciones de trabajo con sus respectivos puntos de acceso a red inalámbricos, desde donde se envían los datos hacia el repositorio central ubicado en la ciudad de Guayaquil.

2.2.2. Muestra.

Para la toma de muestra se ha escogido un muestreo probabilístico estratificado con afijación proporcional de la muestra. En este tipo de diseño la población se segmenta o estratifica en subgrupos según una determinada característica o variable de estratificación y este procedimiento se define de forma proporcional. En el caso de nuestro estudio se tuvo en cuenta las Zonas con un número de haciendas establecidas como variables de estratificación.

La fórmula se describe a continuación:

Determinamos N :

Ecuación 1 Fórmula para determinar la población total

$$\sum_{h=1}^L N_h = N$$

Donde N es el total de individuos de la población, L es el número de sub-poblaciones o estratos en los que se ha dividido a N .

$$N_1 + N_2 + N_3 \dots + N_L = N$$

Determinamos n :

Ecuación 2. Muestra Estratificada

$$\sum_{h=1}^L n_h = n$$

El tamaño muestral total se determina a través de los tamaños muestrales de cada estrato de la población mediante,

$$n_1 + n_2 + n_3 \dots + n_L = n$$

Determinamos k :

Como definimos una afijación proporcional entonces debemos obtener un valor constante k de forma tal que se cumpla:

Ecuación 3. Constante k

$$n_h = kN_h$$

Para determinar el tamaño muestral debemos determinar el valor de k a través de:

Ecuación 4. Valor de constante k

$$k = n/N$$

Determinamos W_h :

Los valores de W_h se pueden obtener mediante:

Ecuación 5. Coeficiente de Ponderación

$$W_h = \frac{n_h}{n}$$

De aquí que podemos calcular los coeficientes de ponderación W_h mediante las variables: n_h y n .

Por lo tanto, analizados todos los elementos que serán necesarios para el cálculo de la muestra proporcional, se presenta la fórmula que se utilizarán, y se tiene que:

Ecuación 6. Calculo de la Muestra Proporcional

$$n_h = n \left(\frac{N_h}{N} \right) = nW_h$$

Ahora, para encontrar cual será la muestra en cada una de las proporciones del universo poblacional se procede a reemplazar valores:

N: 249	Tamaño de la población global objetivo
N_h :	Tamaño de población proporcional
n: 25	Tamaño de la muestra global que se desea obtener
k: 0,1	Coefficiente de proporción

L: 6

Número de estratos

n_h : ?

Ecuación 7. Calculo para encontrar cada muestra proporcional del universo poblacional

$$n_1 = 25 \left(\frac{39}{249} \right) = 25(0,156)$$

$$n_1 = 3,9$$

$$n_2 = 21 \left(\frac{48}{210} \right) = 21(0,228)$$

$$n_2 = 4,7$$

$$n_3 = 16 \left(\frac{66}{162} \right) = 16(0,407)$$

$$n_3 = 6,5$$

$$n_4 = 10 \left(\frac{57}{96} \right) = 10(0,593)$$

$$n_4 = 2,7$$

$$n_5 = 4 \left(\frac{27}{39} \right) = 25(0,692)$$

$$n_5 = 2,7$$

$$n_6 = 1 \left(\frac{12}{12} \right) = 1(1)$$

$$n_6 = 1$$

Se tomará muestra de cada zona, por encontrarse en lugares con infraestructuras diferentes, teniendo un total de 25 host identificados como muestra.

En la tabla N° 3 se muestra un resumen de distribución de los hosts, zonas y porcentajes de los cuales serán obtenidos los datos para el posterior desarrollo de la investigación en curso.

Tabla 3. Cuadro de distribución de muestras.

Estrato	Identificación	Host/Estrato	Proporción	Muestra
1	Zona Norte 1	39	15,70%	4
2	Zona Norte 2	48	19,30%	5

3	Zona Centro 1	66	26,50%	6
4	Zona Centro 2	57	22,90%	6
5	Zona Sur 1	27	10,80%	3
6	Zona Sur 2	12	4,80%	1
Totales:		249	99,80%	25

2.3. Métodos y técnicas empleadas para la recolección de la información

Según la empresa Cisco Systems Inc, el concepto de recolección de la información, encierra todas las técnicas que se utilizan para registrar las observaciones o resultados de los elementos puestos a prueba; los instrumentos, los objetos externos e independientes utilizados; y los recursos, como los medios necesarios para obtener y registrar dicha información. (Cisco Systems, Inc., 2018)

Según varios autores, se clasifica a las técnicas de recolección de información en 6 grandes grupos:

- Observación
- Entrevista
- Pruebas y Test
- Técnicas grupales
- Análisis de documentos

2.3.1. Variables

Tabla 4. Variables

Ítem	Variables	Definición Conceptual	Definición Operacional
1	Texto Plano	Hace mención al archivo original antes de cifrar	Archivo original

2	3DES	Hace mención al archivo cifrado con el algoritmo 3DES	Se cifra el archivo con el algoritmo 3DES
3	RSA	Hace mención al archivo cifrado con el algoritmo RSA	Se cifra el archivo con el algoritmo RSA

VARIABLES QUE SE EVALUARÁN DURANTE LAS PRUEBAS.

2.3.2. Constantes

Tabla 5. Constantes

Ítem	Constante	Definición Conceptual	Definición Operacional
1	Día de realización de las pruebas	Hace mención al día en que se realizaran las pruebas	Se realizaran las pruebas en días de mayor carga de trabajo en las plantas procesadoras
2	Horario de transferencia de archivo	Hace mención al horario en que se realizaran las pruebas	Se realizaran las pruebas en horarios de mayor carga de trabajo en la transferencia de archivos al repositorio
3	Tamaño del archivo original	Hace mención al tamaño del archivo con el que se efectuaran las pruebas	Se realizaran las pruebas con un mismo archivo para evitar resultados afectados.

CONSTANTES EN LAS QUE SE LLEVARA A CABO LAS PRUEBAS.

2.3.3. Parámetros

Tabla 6. Parámetros

Ítem	Parámetros	Acrónimo	Definición Conceptual	Definición Operacional	Dimensiones	Indicador
1	Tiempo de carga de archivo en el repositorio central	TC	Hace mención al tiempo que tarda en subirse el archivo desde el dispositivo Raspberry PI hasta el Repositorio central	Recibo del Ack en el dispositivo Raspberry PI enviado desde el repositorio central	<ul style="list-style-type: none"> El archivo .txt es cifrado en el dispositivo Raspberry El archivo cifrado es enviado al repositorio central utilizando El repositorio central envía al dispositivo Raspberry el acuse de recibo 	Segundos
2	Tamaño del archivo cifrado	TA	Hace mención al aumento de tamaño del archivo después del cifrado en comparación al tamaño original	Se compara el tamaño del archivo plano con el archivo cifrado	<ul style="list-style-type: none"> Tamaño del archivo cifrado en relación al tamaño del archivo original en texto plano 	Kb

Parámetros que serán analizadas durante el proceso de pruebas.

2.4. Procesamiento de la información

Las pruebas se realizarán en 25 hosts ubicados en diferentes localidades, durante horarios y días diferentes, para medir los tiempos de llegada de los archivos cifrados hasta un repositorio central, por ello se realizará todas las pruebas correspondientes en cada uno de los dispositivos Raspberry para obtener una vista más amplia de los resultados.

Actualmente se está subiendo la información en texto plano hasta el repositorio central, lo que permite que cualquier persona que logre conectarse a la intranet, podrá ver la información contenida en el documento.

La información de las empresas es el activo más importante, por lo que, como institución, necesita protegerla, y pensando en esta necesidad, se ha visto obligada a buscar mecanismos que ayuden a ocultar los datos contenidos en el archivo enviado, para que, aunque se pueda ver la información durante el paso de las tramas en su paso por la capa de transporte, no se pueda modificar, leer, o copiar.



The image shows a screenshot of a text editor window displaying a table of test results. The table has 13 columns: a line number, a file ID, a count, a code, a host name, a location, a date and time, and four numerical values. The data is organized in pairs of rows for each host.

Line	File ID	Count	Code	Host	Location	Date/Time	Val1	Val2	Val3	Val4
1	5983296	2	M02122	181049	BNN SHARBATLY VC 31LB	26/04/2018 6:34:02	32,8	31,0	32,8	
2	5983296	2	M02122	181049	BNN SHARBATLY VC 31LB	26/04/2018 6:34:17	32,9	31,0	32,8	
3	5983317	2	M02122	222790	BNN GREENTROP	26/04/2018 6:34:32	33,0	32,9	32,9	
4	5983317	2	M02122	222790	BNN GREENTROP	26/04/2018 6:34:47	31,8	32,9	32,9	
5	5983288	2	M02122	217794	BNN FAVORITA 25CB CGC	26/04/2018 6:35:02	39,9	42,0	44,1	
6	5983288	2	M02122	217794	BNN FAVORITA 25CB CGC	26/04/2018 6:35:17	40,6	42,0	44,1	
7	5983288	2	M02122	217794	BNN FAVORITA 25CB CGC	26/04/2018 6:35:32	40,2	42,0	44,1	
8	5983309	2	M02122	227366	BNN BANINI 43.5LB	26/04/2018 6:35:47	46,6	43,5	43,5	
9	5983309	2	M02122	227366	BNN BANINI 43.5LB	26/04/2018 6:36:02	45,8	43,5	43,5	
10	5983296	2	M02122	181049	BNN SHARBATLY VC 31LB	26/04/2018 6:36:17	32,8	31,0	32,8	
11	5983296	2	M02122	181049	BNN SHARBATLY VC 31LB	26/04/2018 6:36:32	32,9	31,0	32,8	
12	5983317	2	M02122	222790	BNN GREENTROP	26/04/2018 6:36:47	33,0	32,9	32,9	
13	5983317	2	M02122	222790	BNN GREENTROP	26/04/2018 6:37:02	31,8	32,9	32,9	
14	5983288	2	M02122	217794	BNN FAVORITA 25CB CGC	26/04/2018 6:37:17	39,9	42,0	44,1	
15	5983288	2	M02122	217794	BNN FAVORITA 25CB CGC	26/04/2018 6:37:32	40,6	42,0	44,1	
16	5983288	2	M02122	217794	BNN FAVORITA 25CB CGC	26/04/2018 6:37:47	40,2	42,0	44,1	
17	5983309	2	M02122	227366	BNN BANINI 43.5LB	26/04/2018 6:38:02	46,6	43,5	43,5	
18	5983309	2	M02122	227366	BNN BANINI 43.5LB	26/04/2018 6:38:17	45,8	43,5	43,5	
19	5983296	2	M02122	181049	BNN SHARBATLY VC 31LB	26/04/2018 6:38:32	32,8	31,0	32,8	
20	5983296	2	M02122	181049	BNN SHARBATLY VC 31LB	26/04/2018 6:38:47	32,9	31,0	32,8	
21	5983317	2	M02122	222790	BNN GREENTROP	26/04/2018 6:39:02	33,0	32,9	32,9	
22	5983317	2	M02122	222790	BNN GREENTROP	26/04/2018 6:39:17	31,8	32,9	32,9	
23	5983288	2	M02122	217794	BNN FAVORITA 25CB CGC	26/04/2018 6:39:32	39,9	42,0	44,1	
24	5983288	2	M02122	217794	BNN FAVORITA 25CB CGC	26/04/2018 6:39:47	40,6	42,0	44,1	
25	5983288	2	M02122	217794	BNN FAVORITA 25CB CGC	26/04/2018 6:40:02	40,2	42,0	44,1	
26	5983309	2	M02122	227366	BNN BANINI 43.5LB	26/04/2018 6:40:17	46,6	43,5	43,5	
27	5983309	2	M02122	227366	BNN BANINI 43.5LB	26/04/2018 6:40:32	45,8	43,5	43,5	
28	5983296	2	M02122	181049	BNN SHARBATLY VC 31LB	26/04/2018 6:40:47	32,8	31,0	32,8	
29	5983296	2	M02122	181049	BNN SHARBATLY VC 31LB	26/04/2018 6:41:02	32,9	31,0	32,8	
30	5983317	2	M02122	222790	BNN GREENTROP	26/04/2018 6:41:17	33,0	32,9	32,9	
31	5983317	2	M02122	222790	BNN GREENTROP	26/04/2018 6:41:32	31,8	32,9	32,9	
32	5983288	2	M02122	217794	BNN FAVORITA 25CB CGC	26/04/2018 6:41:47	39,9	42,0	44,1	
33	5983288	2	M02122	217794	BNN FAVORITA 25CB CGC	26/04/2018 6:42:02	40,6	42,0	44,1	
34	5983288	2	M02122	217794	BNN FAVORITA 25CB CGC	26/04/2018 6:42:17	40,2	42,0	44,1	
35	5983309	2	M02122	227366	BNN BANINI 43.5LB	26/04/2018 6:42:32	46,6	43,5	43,5	
36	5983309	2	M02122	227366	BNN BANINI 43.5LB	26/04/2018 6:42:47	45,8	43,5	43,5	

Figura 7. Archivo enviado en texto plano.

Como se puede apreciar en la figura N° 7, la información es completamente legible y por lo tanto susceptible de ser modificada, lo que comprometería su integridad, uno de los principios básicos de la seguridad en la información.

Este mismo archivo con toda su información, se la analizó con Wireshark durante su paso por la capa de transporte, y se pudo verificar que el texto que contenía se podía leer con facilidad como se muestra a continuación.

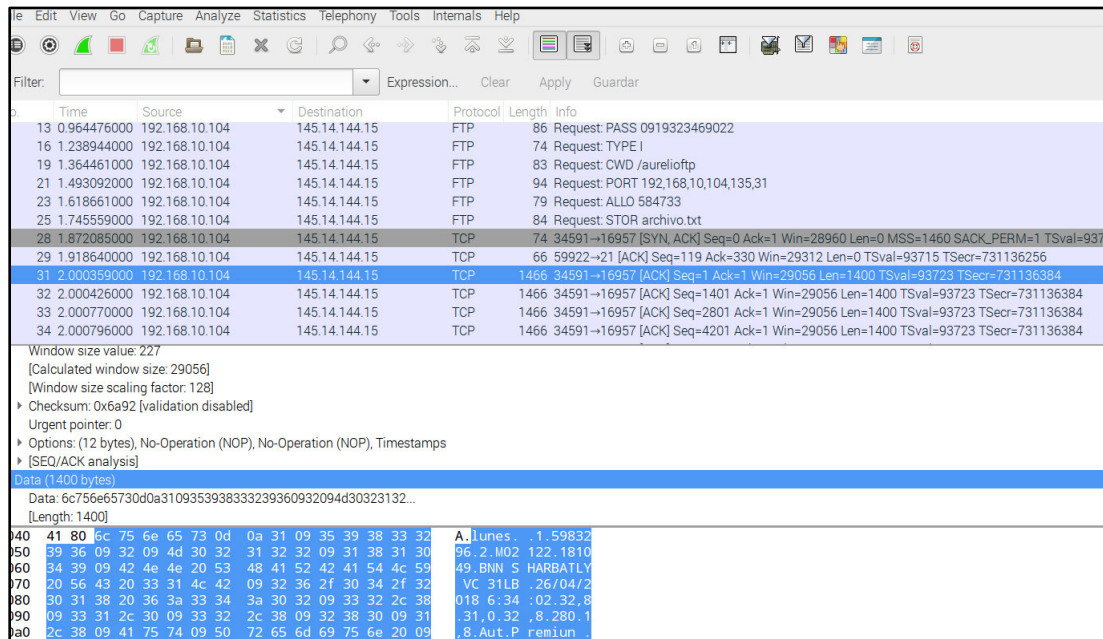


Figura 8. Captura de trama con Wireshark al archivo en texto plano.

Como se muestra en la figura N° 8, la palabra “Lunes” que fue puesta como indicador, se presenta al principio del bloque de la trama, viniendo después los datos reales del archivo analizado.

Como se ve a continuación, no solo se puede ver el contenido del archivo, sino también otros parámetros necesarios al enviar la información como datos de acceso, como usuario y contraseña, directorios de archivo y las direcciones de IP.

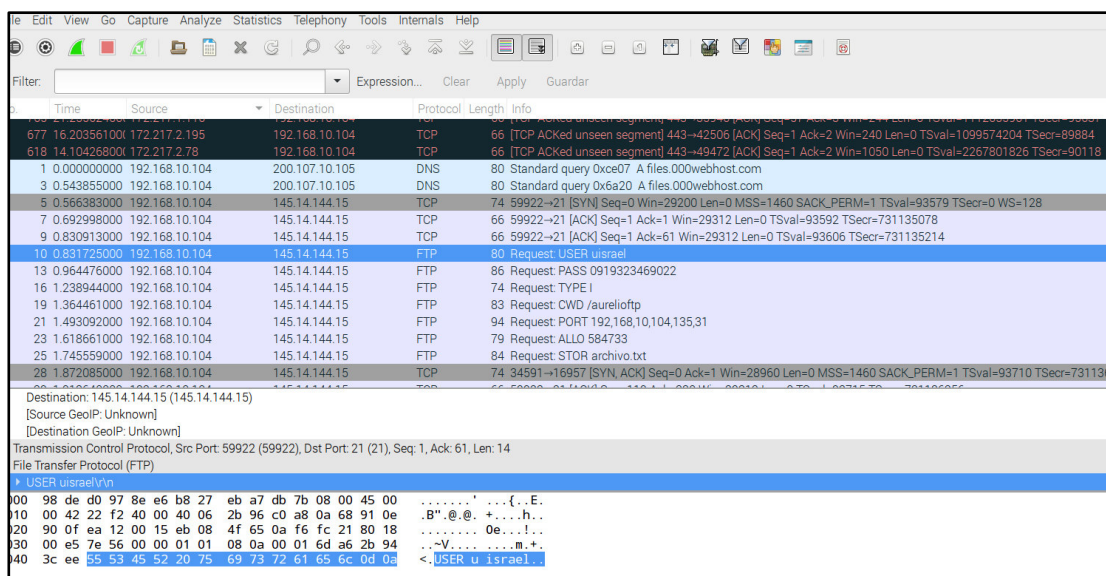


Figura 9. Datos de usuario

La figura N° 10, muestra la información de acceso, en un formato legible, lo que permite a cualquier usuario apropiarse de las credenciales y dar cualquier uso.

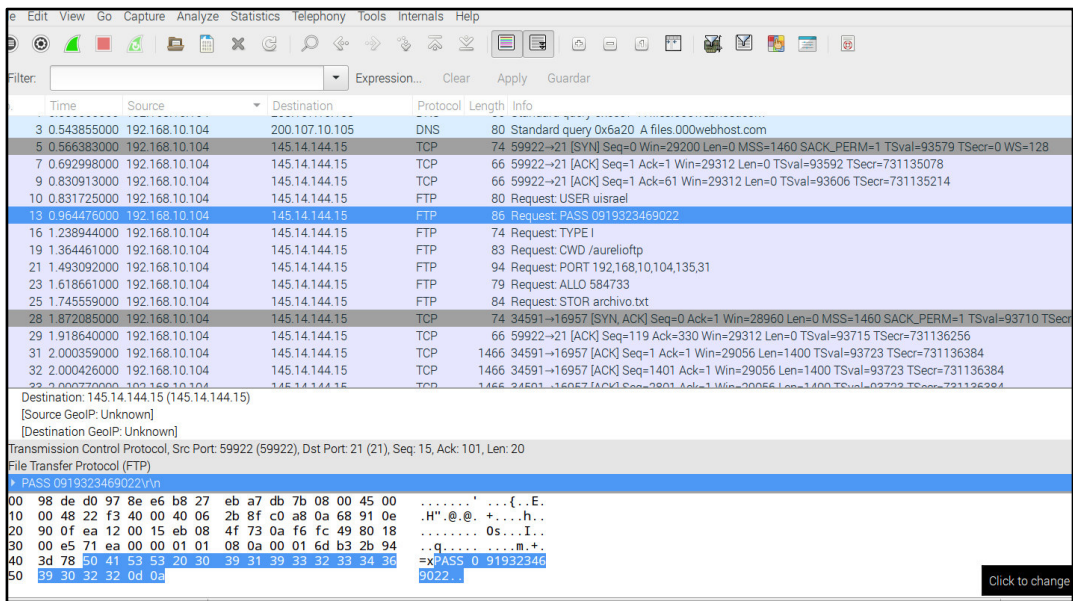


Figura 10. Datos de usuario.

Se muestra la contraseña, necesaria para acceder al repositorio.

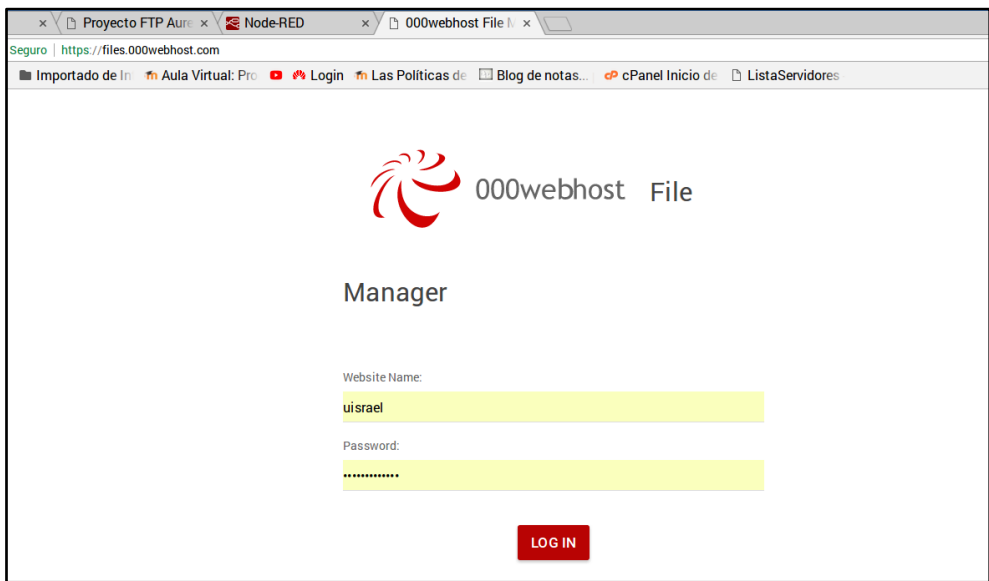


Figura 11. Formulario de acceso al Repositorio Central.

En la figura N° 11, se muestra los datos de usuario y contraseña necesarios para el acceso al repositorio, que son los mismos datos que se visualizan con Wireshark durante el análisis de la red.

Se necesita un mecanismo criptográfico que cifre la información contenida en el archivo, de manera que la información se encuentre segura durante su paso por la capa de transporte, por lo que se analizarán 2 algoritmos de cifrado que hagan ilegible la información, sin que se comprometa otros recursos.

Además, se procesará la información en una hoja de cálculo, donde se facilitará la posterior revisión y análisis, presentando gráficos estadísticos y cuadros comparativos de manera práctica y secuencial de toda la información obtenida durante el proceso de investigación.

2.4.1. Recolección de la Información

La recolección de información se da como resultado de los datos obtenidos, durante el proceso de pruebas en cada una de los hosts de cada zona. Esta información es recolectada en fichas técnicas que después son tabuladas en hojas de cálculo para su respectivo análisis.

Las fichas de observación estarán diseñadas para almacenar toda la información concerniente a las estaciones de trabajo donde se realizarán las pruebas, tanto a la ubicación del host como los resultados emitidos en las pruebas.

2.5. Metodología Aplicada

La metodología utilizada para la realización de la actual investigación, está basado en un enfoque cuantitativo con un diseño experimental, midiendo independientemente las variables definidas anteriormente, con el fin específico de describir las propiedades dichos resultados.

Debido a que la investigación se encuentra conectada en todas sus fases de manera lógica y secuencial se puede verificar periódicamente la contrastación que existe entre sus procesos, de manera que se podrá al finalizar la investigación, cuantificar los resultados obtenidos.

2.6. Herramientas y Materiales

Entre las herramientas que se utilizarán se puede nombrar:

- Wireshark
- Linux (Debian)
- Raspberry PI3
- PC portátil, teclados, mouse y libretas, cuadernos, lápices y esferos

CAPÍTULO III

PROPUESTA Y DISEÑO

3.1. Fundamentos del proyecto

Basado en estudios realizados en varias tesis e investigaciones realizadas por otros autores, se ha podido encontrar que, a pesar de haberse realizado varios estudios comparativos entre metodologías criptográficas en entornos con infraestructura robusta, refiriéndose a equipos con características que superan las 4 Gb de memoria RAM y procesadores de última generación; no se han realizados estos mismos estudios investigativos sobre una infraestructura con recursos limitados.

Continuando con lo anterior expuesto, siendo un microcomputador de placa única, con un procesador de 1.2GHz de 64bit y una memoria de 1Gb, la Raspberry PI3 se convierte en el dispositivo ideal para realizar la investigación antes mencionada.

La empresa agrícola en la que serán realizadas las pruebas, cuenta con toda una infraestructura apostada con Raspberry PI3 en sus instalaciones de proceso, las cuales están en proceso de prueba, con un software basado en Linux, con SO Debian, y con una red inalámbrica.

Para verificar el paso del archivo por la red inalámbrica y su contenido durante la transferencia, Wireshark es uno de los analizadores de protocolo ideales, ya que ayuda verificando no solo el paso del archivo sino también factores como el de la seguridad de la información.

3.2. Presentación del proyecto

Para la realización de la presente investigación se utilizará una plataforma tecnológica con dispositivos con características limitadas, microcomputadores de placa única que se encontraran formando parte de redes inalámbricas que se conectan a un repositorio central, donde se verificará la información enviada.

Con el analizador de protocolos se verificará los datos mientras están siendo enviados por la capa de transporte, comprobando el estado en que se encuentra, tanto en formato cifrado como en formato de texto plano, y su contenido.

3.2.1. Plataforma Tecnológica

Se procederá a realizar las pruebas de toma de datos en cada una de las respectivas empacadoras, de cada hacienda, en cada zona; efectuando 3 envíos desde el dispositivo Raspberry PI3 hasta el repositorio central, para luego de promediar, registrar dicho valor.

Se medirá el tiempo que tarde el envío del archivo desde el dispositivo hasta llegar a un repositorio en la nube, tanto como texto plano, como cifrado con 3DES y RSA. En el transporte se verificará con Wireshark los datos del archivo, encabezado y valores de usuario y contraseña.

Adicionalmente a lo antes mencionado, se analizará la calidad de cifrado de los algoritmos sometidos a prueba y por último, el porcentaje de crecimiento del archivo luego de haber sido cifrado con relación al archivo original.

Los resultados serán presentados individualmente, por zona y globalmente, tanto en valores numéricos como en gráficos estadísticos que faciliten su comprensión y análisis.

3.2.2. Planimetría Zonal

Con el fin de alcanzar una geolocalización de las zonas y como están distribuidas a nivel nacional, se presenta a continuación sus ubicaciones a lo largo de las 5 provincias del país, además de la distribución según el proveedor del servicios de enlace de última milla.

Aunque el proveedor del servicio de internet es uno solo, “Claro”, existen 2 proveedores diferentes que están brindando el servicio de enlaces de última milla (Nivel físico, antenas, radios, etc.), en la figura N° 12 se puede ver que las zonas norte 1 y norte 2 están cubiertas por el proveedor del servicio de enlaces “Skyweb”, mientras que las demás zonas están con “Transdatel”.

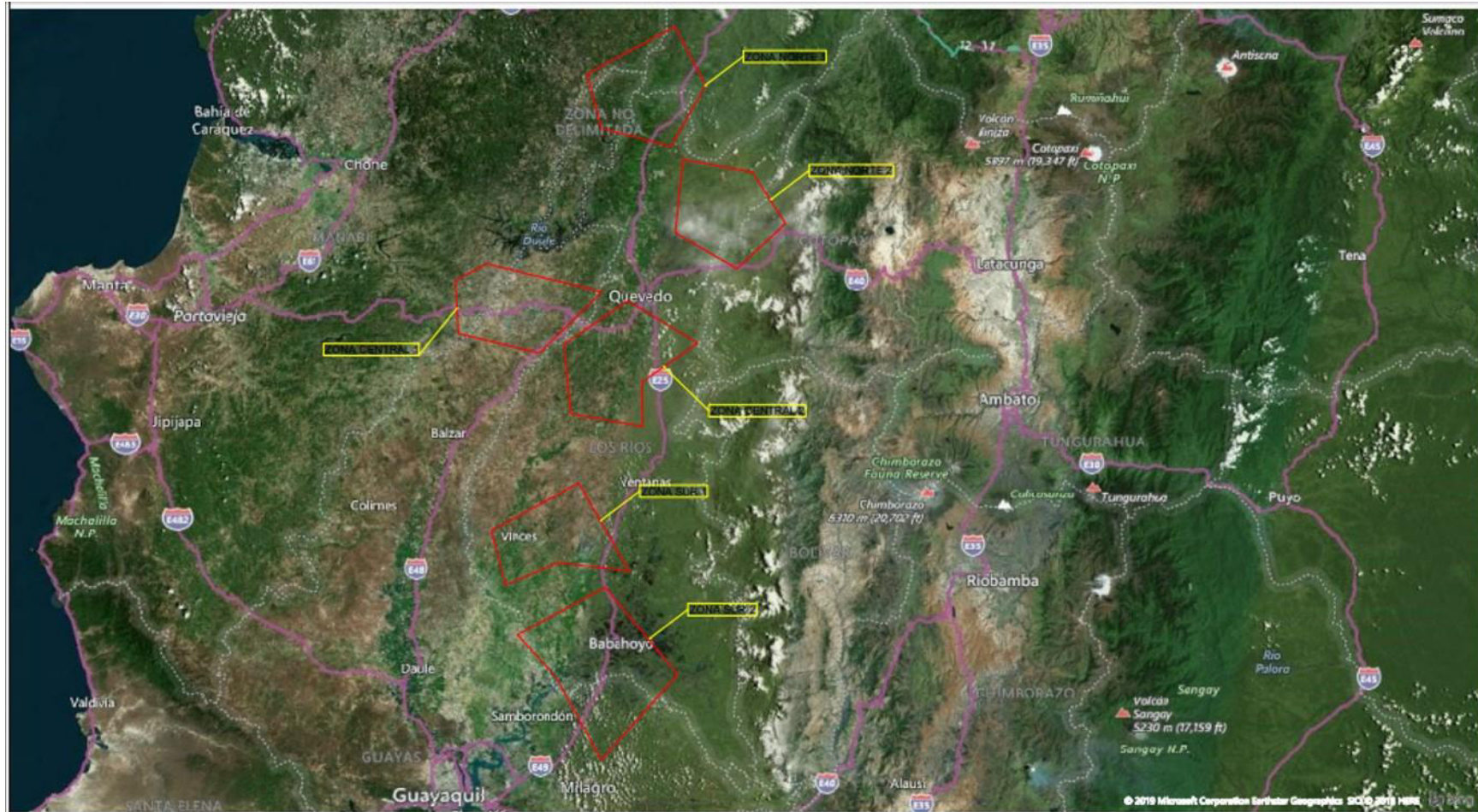


Figura 12. Mapa de Planimetría Zonal.

Es importante además, indicar que las zonas Norte 1 y Norte 2 mantienen un ancho de banda de 2 megas, mientras que las demás zonas están saliendo con un ancho de banda de 6 megas, y a pesar de que anteriormente no presentaban problemas de enlaces en las zonas Norte 1 y 2, desde que se está trabajando con el SBE sí se han estado presentando ciertos inconvenientes con varios usuarios con respecto a este tema.

3.2.3. Archivo enviado desde Dispositivos Raspberry PI

El archivo que se enviara desde los dispositivos Raspberry PI3 hasta el repositorio central, estarán siendo enviados en dos formatos diferentes:

- Texto Plano.** En este formato será legible la información contenida, siendo posible la lectura de la información del archivo.
- Texto cifrado.** En este formato la información contenida estará cifrada tanto con RSA como con 3DES, lo que imposibilitará la comprensión de los datos enviados.

En el archivo original, sin cifrar, se encontrarán 2500 registros de cajas pesadas con todos sus componentes que lo integran, que es un promedio de las cajas que se procesan en todas las empacadoras diariamente, además, tendrá un tamaño de archivo de 572 Kb. Y será enviado desde cada uno de los hosts que se encuentran en las empacadoras, desde donde se enviaran hasta el repositorio central.

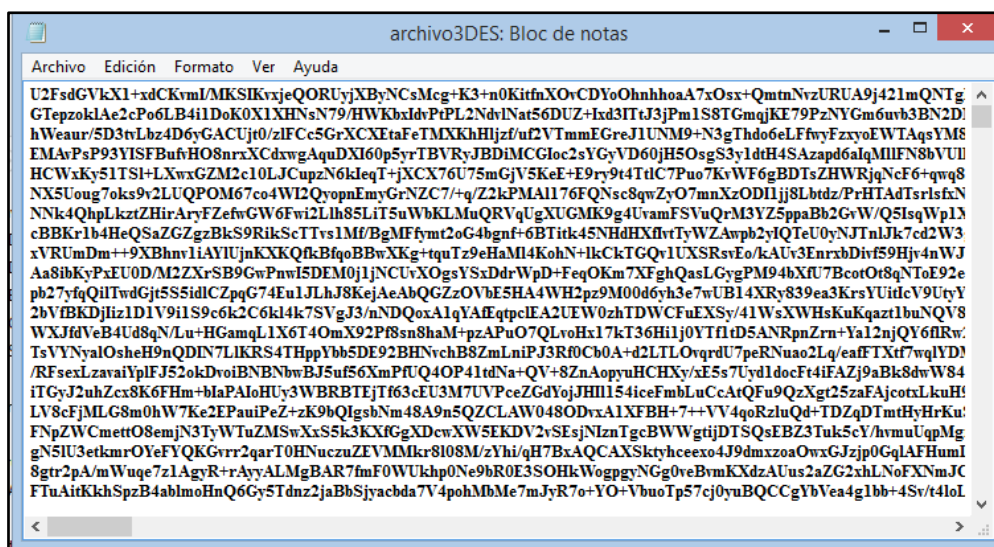


Figura 13. Archivo de texto cifrado con 3 DES

Como se muestra en la figura 13, el archivo cifrado con 3DES, será el mismo archivo en texto plano que luego de ser procesado con el algoritmo 3DES se convertirá en un archivo encriptado, que será ilegible durante su paso por la capa de transporte, y su tamaño variará dependiendo de los resultados del proceso de cifrado.

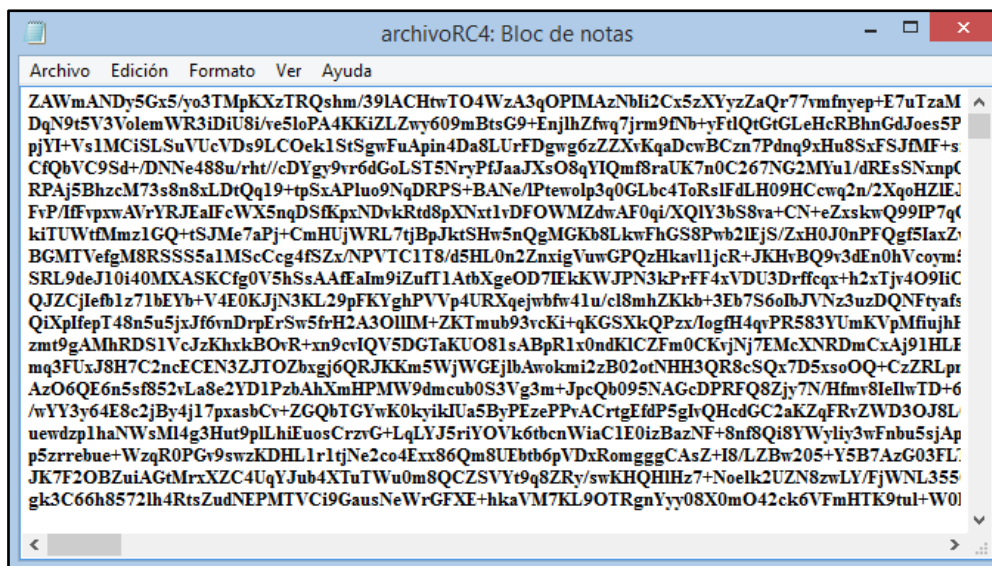


Figura 14. Archivo de texto cifrado con RSA

De igual manera, como se muestra en la figura N° 14, el archivo cifrado con RSA, será el archivo original que se cifrara, y su tamaño también variará dependiendo de los resultados del proceso de cifrado. Estos archivos estarán siendo monitoreados durante su paso por la capa de transporte por el analizador de protocolos Wireshark, con el cual se verificará su contenido, además de otros parámetros.

3.2.4. Analizador de Protocolos

Con Wireshark se procede a monitorear la red donde se están realizando las pruebas, capturando tramas donde está localizada la información que se está enviando, y se visualiza la siguiente información:

3.2.4.1. Análisis del archivo en texto cifrado

A continuación se presentan las capturas de las tramas durante el envío de los archivos cifrados con los respectivos algoritmos.

Según lo que se visualiza en la figura N° 15, Wireshark muestra la información contenida en el archivo de texto, pero por encontrarse esta información cifrada se hace imposible su comprensión.

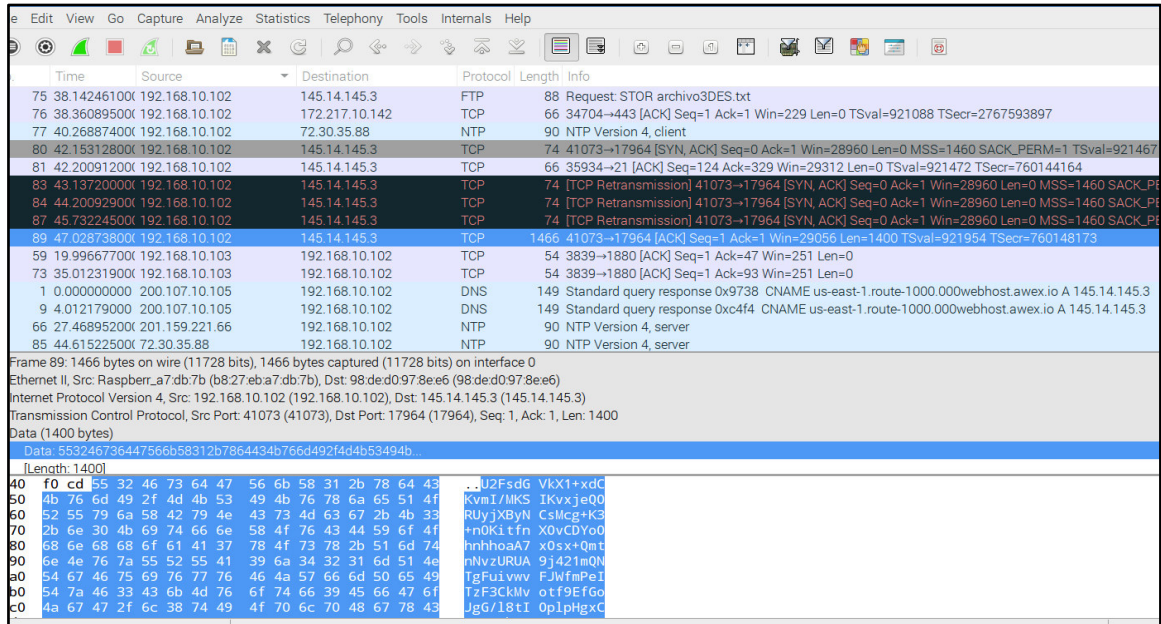


Figura 15. Captura con Wireshark del archivo cifrado con 3DES.

Continuando con lo anterior, no es suficiente con cifrar el contenido de la información incluida en el archivo de texto, sino también toda la demás información concerniente como directorios de archivos, direcciones IP, y datos de acceso como usuario y contraseña.

En la figura N° 16 se muestra como ejemplo una captura con Wireshark de una aplicación web donde se está manteniendo cifrada toda esta información anteriormente nombrada, y se puede ver como se ha utilizado algoritmos de cifrado combinados para alcanzar un grado de seguridad aún mayor.

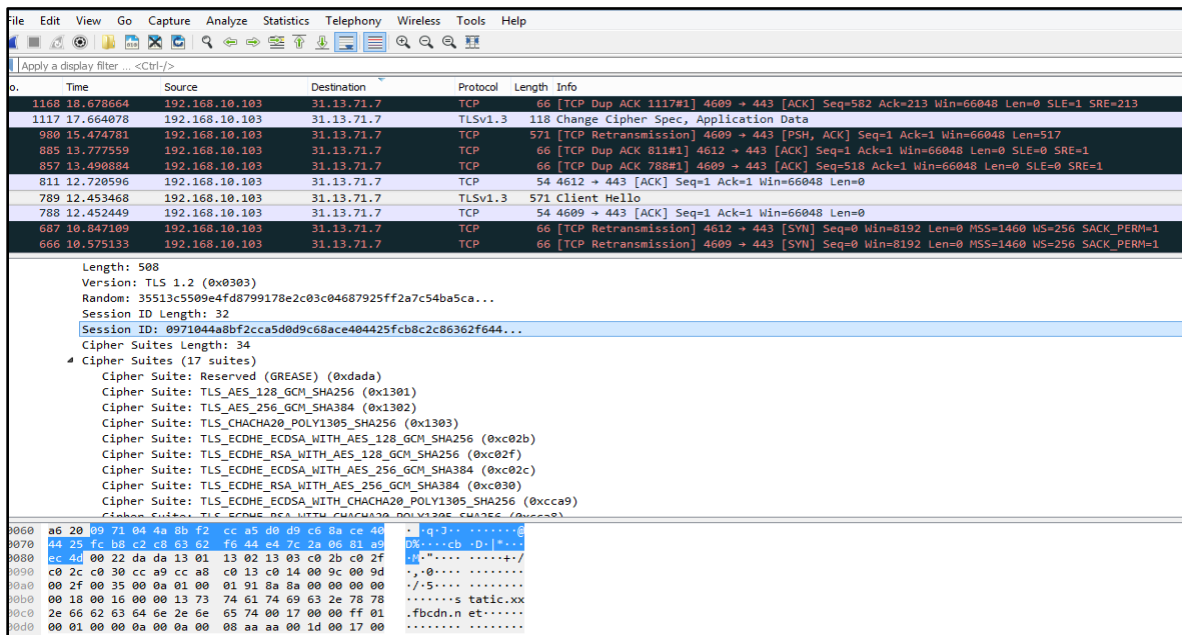


Figura 16. Ejemplo de página cifrada con AES y RSA

3.2.5. Políticas de Seguridad

La ISO 27001:2013 es la única norma susceptible de auditoría que define los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI), estando pensada para garantizar la selección de controles adecuados.

Los dominios de la norma ISO/IEC 27001:2013 corresponden a los diferentes capítulos que establecen los requerimientos que las organizaciones deben cumplir para el establecimiento de un Sistema de Gestión de Seguridad de la Información, de los cuales se va a enfocar en el que compete, de acuerdo con la presente investigación.

Continuando con lo anterior, la investigación se va a centrar en el anexo A de la ISO 27001:2013, donde se encuentran los 39 objetivos de control y 133 controles, agrupados en 11 dominios, y más específicamente en el dominio número 10: Cifrado, controles criptográficos.

La ISO 27002:2013 es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información, para el tratamiento de controles criptográficos se va a revisar sus 2 controles:

a. Políticas de uso de los controles criptográficos

Se deberá desarrollar e implantar una política de uso de controles criptográficos para la protección de las llaves o claves de cifrado.

A continuación, se detalla un fragmento de una plantilla donde constan los principales controles a considerar para nuestra política, aplicada a la empresa donde se obtuvieron las muestras.

Especificación

Control

Las claves secretas utilizadas para cifrado simétrico, también llamada criptografía de clave simétrica, deben de estar protegidas mientras se distribuyen a todas las partes que las van a utilizar.

Durante la distribución de claves secretas se debe de utilizar cifrado simétrico, las claves de cifrado simétrico para envío deben de utilizar el algoritmo más fuerte especificado en la política de cifrado aceptable de la empresa, con la clave de la longitud más larga permitida.

Claves secretas para cifrado simétrico

Si las claves de cifrado simétrico son para cifrar un algoritmo más fuerte, entonces las claves para envío deben de dividirse, cada parte de la clave de cifrado a enviar con una clave de cifrado simétrico diferente que sea de la longitud de clave más larga autorizada y después cada porción cifrada se transmite utilizando diferentes mecanismos de transmisión. El objetivo es proporcionar la protección más rigurosa a la clave en el envío que a los datos que se cifraran con esa clave de cifrado.

Las claves para cifrado simétrico, cuando están en reposo, deben de estar protegidas con medidas de seguridad al menos tan estrictas como las medidas utilizadas para la distribución de esa clave.

Llaves de cifrado de PKI

La criptografía de llave pública o la criptografía asimétrica, utiliza pares de llaves públicas y privadas. La llave pública se pasa a la autoridad de certificación para ser incluida en el certificado digital emitido para el usuario

final. El certificado digital está disponible para todo el mundo una vez emitido. La llave privada sólo debe estar disponible para el usuario final al que se expide el certificado digital correspondiente.

Los pares de llaves pública y privada emitidas por la infraestructura de llave pública (PKI) de la empresa se generan en Smart Cards reforzadas emitidas a un usuario final específico. La llave privada asociada con el certificado de identidad de un usuario final, que sólo se utiliza para las firmas digitales, nunca deberá de salir de la Smart Card, esto evita que el equipo de TecnoSegIsrael guarde la llave en el depósito en garantía cualquier llave privada relacionadas con los certificados de identidad. La llave privada asociada con algún certificado de cifrado, que se utiliza para cifrar correo electrónico y otros documentos, debe de estar custodiada en el depósito en garantía en cumplimiento de las políticas de la empresa.

El acceso a las llaves privadas almacenadas en una Smart Card emitida por la empresa estará protegido por un número de identificación personal (PIN) que sólo es conocida por el individuo a quien se emite la Smart Card. El software de la Smart Card será configurado para requerir la introducción del PIN antes acceder a cualquier llave privada contenida en la Smart Card que se está accediendo.

En los anexos se encuentra la política completa.

b. Gestión de claves

Se debería establecer una gestión de las claves que respalde el uso de las técnicas criptográficas en la Organización.

Una opción para la gestión de claves es KeePass, por estar bajo código libre y con licencia GNU GLPv2 está disponible para plataformas Linux, puede instalar la edición portátil de KeePass en una unidad de disco USB y guardarla en su bolsillo. No escribe ningún dato fuera de esa unidad, por lo que puede usarlo en cualquier computadora.



Figura 17. Configuración del Generador de Contraseñas Seguras de KeyPass

La figura N° 17 muestra un ejemplo de una contraseña segura, utilizando caracteres alfanuméricos y caracteres especiales, de manera que la variante de búsqueda por diccionario del método de ataque por fuerza bruta no sea viable.

KeePass utiliza un inusual sistema de clave maestra compuesta que puede usar cualquiera o todos los tres métodos de autenticación distintos: contraseña maestra, archivo de clave y cuenta de usuario de Windows

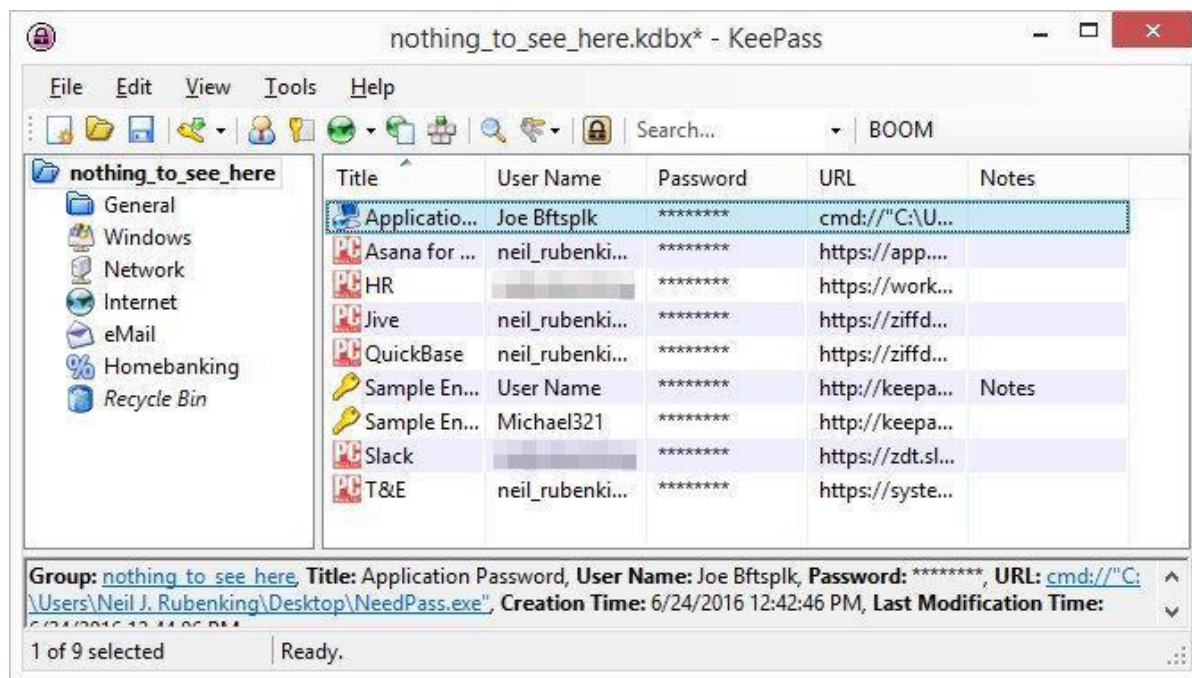


Figura 18. Pantalla de Gestión de Contraseñas con KeyPass

En la figura N° 18 se poder ver que las contraseñas deben ser largas y complejas. No necesariamente deben ser memorizadas, la mayoría de los administradores de contraseñas incluyen un generador de contraseñas, pero muchos de ellos utilizan valores predeterminados deficientes. Norton, utiliza de forma predeterminada contraseñas alfanuméricas de ocho caracteres; Dashlane ofrece contraseñas de 12 caracteres de forma predeterminada, y Enpass Password Manager 5 tiene un máximo de 18 caracteres. KeePass, ofrece una contraseña predeterminada de 20 caracteres, lo que lo convierte en una buena opción.

3.3. Análisis Comparativo entre Tecnologías de cifrado

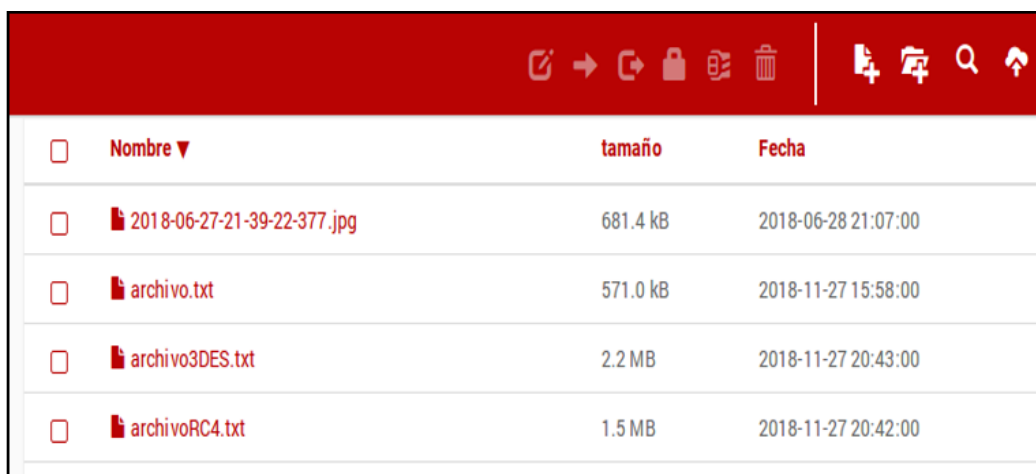
Una vez realizadas las pruebas, se han ingresado los datos registrados en el trabajo de campo en sus respectivas fichas, y se presentan los resultados tabulados de la siguiente manera en cuanto al tiempo de carga del archivo de texto hasta el repositorio central y el crecimiento del tamaño.

3.3.1. Tamaño del archivo

Generalmente después de cifrar cualquier documento, es normal que se genere un ligero crecimiento de tamaño en el archivo original, y ese aumento en el tamaño del documento es importante que sea considerado por cuanto mientras más grande sea el archivo, más tiempo tardará en ser transferido desde el host hasta el repositorio.

Por lo expuesto en el párrafo anterior se ha considerado necesario describir los resultados en cuanto al tamaño de archivo original y después de ser cifrado, luego de realizar las respectivas pruebas, por lo que se encontró el siguiente resultado que se describe a continuación:

En la figura N° 19 se puede notar los tamaños de los archivos en el repositorio, tanto sin cifrar como después de haber sufrido el proceso de cifrado, lo que demuestra el incremento en el tamaño del archivo que es mayor por parte del cifrado 3DES sobre RSA.



<input type="checkbox"/>	Nombre ▼	tamaño	Fecha
<input type="checkbox"/>	2018-06-27-21-39-22-377.jpg	681.4 kB	2018-06-28 21:07:00
<input type="checkbox"/>	archivo.txt	571.0 kB	2018-11-27 15:58:00
<input type="checkbox"/>	archivo3DES.txt	2.2 MB	2018-11-27 20:43:00
<input type="checkbox"/>	archivoRC4.txt	1.5 MB	2018-11-27 20:42:00

Figura 19. Resultado de prueba de tamaño de archivo

Además de que el cifrado con RSA haya conseguido ser de menor tamaño, es importante indicar que por ser un cifrado asimétrico, el nivel de seguridad será también mayor al de un mecanismo de cifrado simétrico como lo es 3DES, sin dejar de nombrar que menor tamaño de archivo supone también menor carga de proceso para el dispositivo.

En la figura N° 20 se visualiza como el cifrado con RSA se muestra de menor tamaño que el cifrado con 3DES, a pesar de ser de mayor tamaño al archivo original, sería una buena opción al momento de decidir por un mecanismo de cifrado, debido a que, lo que se busca es proteger la información en uno de sus pilares básicos de la seguridad, como lo es la integridad.

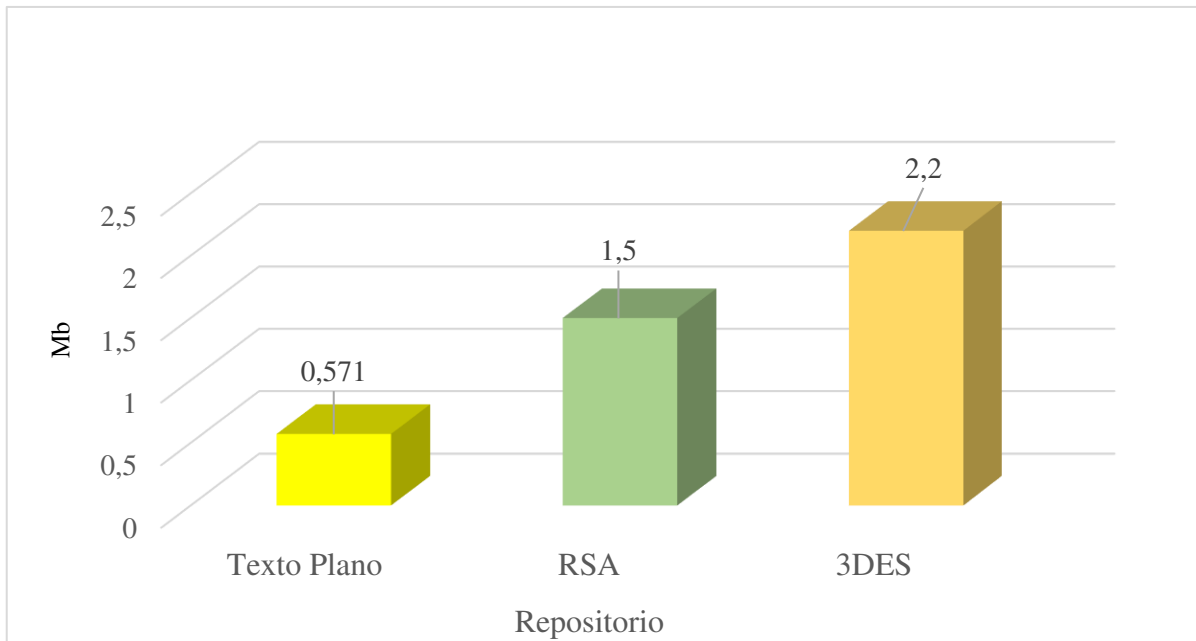


Figura 20. Tamaños de Archivo en Texto Plano y Cifrado

Analizar el tamaño del archivo luego del proceso de cifrado es necesario e importante, debido a que éste influirá directamente en el tiempo que tome desde el envío hasta su llegada en el repositorio. Obviamente, a mayor tamaño, mayor tiempo.

Como se observa en la tabla N° 6, el archivo original que tenía un tamaño de 571 Kb, después del proceso de cifrado con el algoritmo RSA ha aumentado a 1,523 Kb, es decir un crecimiento del 167%; mientras que el mismo archivo en texto plano después del proceso de cifrado con el algoritmo 3DES ha alcanzado los 2,285 Kb, es decir, un crecimiento del 300%.

Tabla 7 Tamaño del archivos transmitido al Repositorio.

Archivo	Variables	Tamaño del Archivo (Kb)
	Texto Plano	571
Archivo	RSA	1,523
	3DES	2,285

Resultados de la variación del tamaño del archivo antes y después de haber sido cifrado con ambos algoritmos.

3.3.2. Tiempo de Carga de Archivo

Los 25 host que constaran como muestra, están localizados en 6 zonas, de donde se tomaran las pruebas, y están ubicadas a lo largo de 4 provincias de la costa y 1 provincia de la sierra del país, además, se cuenta con 2 proveedores diferentes, el primero para las 2 zonas nortes y el segundo para las demás zonas.

Se inicia el proceso de recolección de datos con las 2 zonas nortes, luego con las 2 zonas centro y al final con las 2 zonas sur, completando así las 6 fichas de observación, además, la planimetría zonal se muestra en el párrafo anterior donde se visualiza la ubicación de cada una de las zonas y su correspondiente proveedor del servicio de transporte de datos.

Resultados por Zona:

3.3.3. Zona Norte 1

Se ha realizado una captura de pantalla del momento en que se recibió el mensaje de recibido de parte del repositorio de pruebas, tanto de la transferencia en texto plano como cifrado con RSA y 3DES, además de registrar los resultados físicamente en las fichas de observación.

En la figura N° 21 se muestra la captura con los tiempos del momento en que se confirma el acuse de recibo por parte del repositorio, en la parte superior está el tiempo del envío del archivo en texto plano con 26,94 segundos, en la parte inferior están los tiempos de envío tanto del algoritmo RSA que se está utilizando para las pruebas con 54,44 segundos, y de 3DES que esta con 80,33 segundos, y se puede confirmar los datos presentados en la tabla N°7, donde RSA creció un 102% y 3DES 198% sobre el archivo de texto plano.



Figura 21. Resultados de tiempo de carga Host N° 1

En la figura N° 22 se confirman los datos del host N°2 de la tabla N°7, mientras la transferencia del archivo con texto plano tardó 28,79 segundos, RSA se muestra con un tiempo de 57,05 segundos que representa el 98% de aumento en el tiempo de respuesta, y 3DES con 132,88 segundos, que representa el 362% de aumento en tiempo de respuesta sobre el archivo de texto plano.



Figura 22. Resultados de tiempo de carga Host N° 2

En la figura N° 23 se muestra el envío del archivo desde el host N° 3 de la tabla N°7, donde el archivo en texto plano tardó 31,37 segundos en reportarse recibido, mientras que el archivo enviado con el cifrado RSA tardó 57,9 segundos, con un incremento de tamaño del en un 85%, y del cifrado con 3DES de un 337% de incremento en el tiempo de respuesta con 136,98 segundos.



Figura 23. Resultados de tiempo de carga Host N° 3

En la figura N° 24 se muestra el envío del archivo desde el host N° 4, donde el enviado en texto plano reportó 31,47 segundos, mientras el archivo con el cifrado RSA se reportó en 61,03 segundos, lo que representa un 94% de incremento en el tiempo de respuesta, y del archivo cifrado con 3DES en 121,69 segundos, llegando a alcanzar un 287% de aumento en tiempo de respuesta sobre el archivo en texto plano.

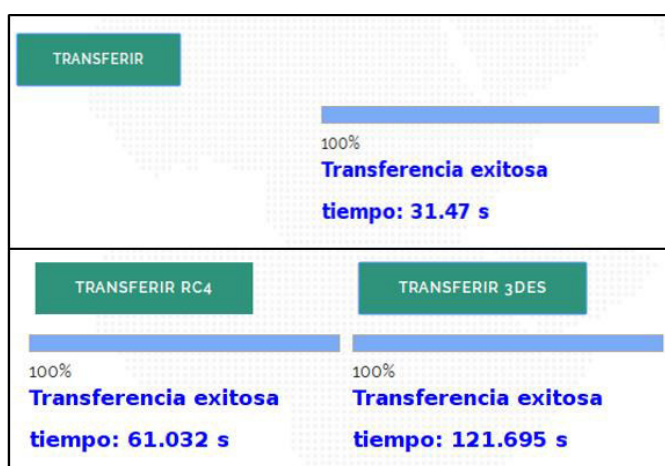


Figura 24. Resultados de tiempo de carga Host N° 4

Resumiendo los resultados obtenidos en la zona norte 1, se tiene que presentan datos muy regulares, y considerando que el proveedor está ofreciendo 2 megas de velocidad, se puede visualizar que RSA está siendo hasta ahora más rápido en presentar el acuse de recibido.

A continuación se presenta la tabla N°7, donde se evidencia los resultados de una manera comparativa, y posteriormente se representan estos mismos datos mediante un gráfico.

Tabla 8. Zona Norte 1

Host	Variables	Tiempo de Carga
Host 1	Texto Plano	26,94
	RSA	54,44
	3DES	80,33
Host 2	Texto Plano	28,79
	RSA	57,05
	3DES	132,88
Host 3	Texto Plano	31,37
	RSA	57,9
	3DES	136,98
Host 4	Texto Plano	31,47
	RSA	61,03
	3DES	121,69

Ficha de recolección de datos N° 1

Se puede apreciar en la tabla N° 7 los resultados de la zona Norte 1 que está compuesta por 4 dispositivos, donde los resultados de las pruebas de tiempo de carga del archivo se muestran en texto plano, cifrados con RSA y con 3DES, y son evidentes en sus tendencias.

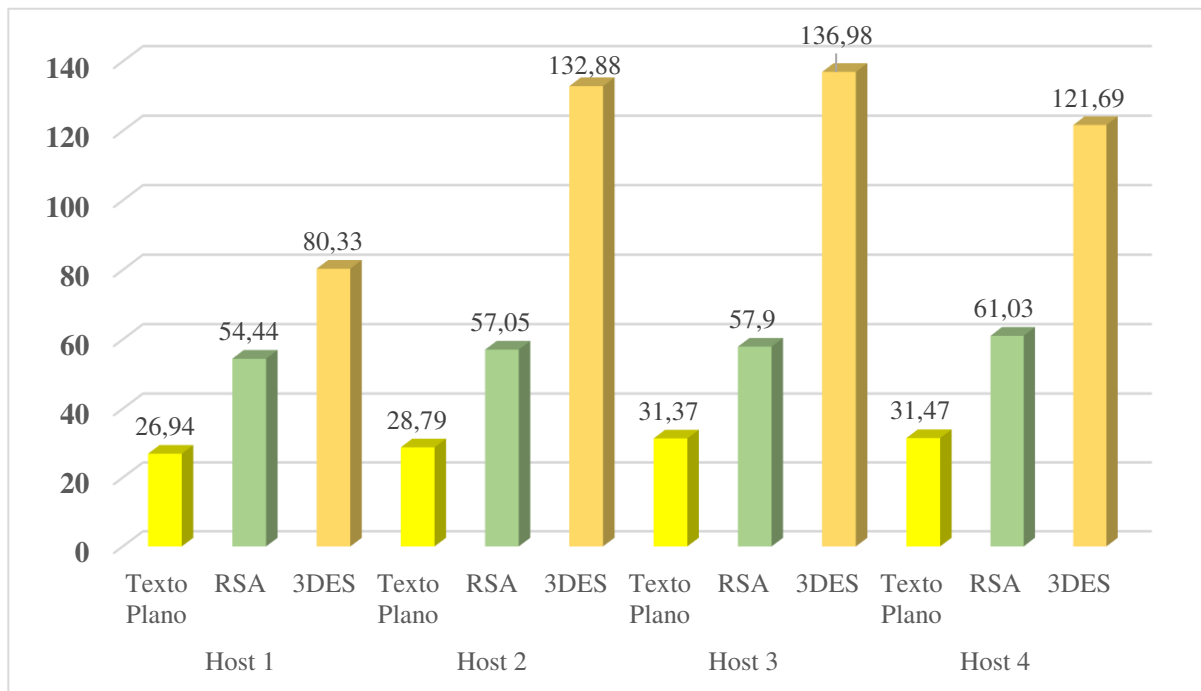


Figura 25. Resumen Tabla N° 8 de Zona Norte 1

La figura N° 25 muestra los valores de la tabla N° 7 en un gráfico de barras, donde se puede visualizar los 4 host, cada uno con sus respectivos tiempos de carga del archivo tanto en formato de texto plano, cifrado con RSA y cifrado con 3DES, y se observa muy marcada la diferencia que existe entre los resultados obtenidos de los algoritmos de cifrados propósitos de prueba.

3.3.4. Zona Norte 2

Claramente se puede notar que el archivo cifrado con el algoritmo 3DES supera por mucho en el tiempo de envío hasta el repositorio al archivo cifrado con el algoritmo RSA, y se demuestra en cada caso, en cada uno de los hosts.

La figura N° 26 muestra la captura en la parte superior del envío del archivo en texto plano desde el host N° 1 de la zona norte 2 con un tiempo de 32,6 segundos, y en la parte inferior se muestra al algoritmo RSA con tiempo de respuesta del enviado de 62,35 segundos que representa un aumento del 91%, y del cifrado con 3DES con 76,85 segundos que representan un 136% de crecimiento, ambos contra el archivo de texto plano.



Figura 26. Resultados de tiempo de carga Host N° 1

La figura N° 27 muestra el envío de los archivos desde el host N° 2 de la zona norte 2, con un tiempo de envío del archivo en texto plano de 40,62 segundos, mostrando incrementos de tamaño del archivo enviado con el cifrado RSA con 72,72 segundos en un 79% y del cifrado con 3DES con 130,33 segundos en un 221%, ambos con respecto del tiempo de envío del archivo en texto plano.



Figura 27. Resultados de tiempo de carga Host N° 2

La figura N° 28 muestra el envío del archivo desde el host N° 3 de la zona norte 2, con un tiempo de 40,83 segundos en el envío del archivo en texto plano, con un incremento de tiempo de envío con el cifrado RSA en un 91% con 77,9 segundos y del cifrado con 3DES de un 213% con 127,79 segundos, ambos en relación al envío en texto plano.



Figura 28. Resultados de tiempo de carga Host N° 3

La figura N° 29 muestra los tiempos de envío de los archivos desde el host N° 4 de la zona norte 2, mostrando el tiempo de envío en texto plano con 67,61 segundos, y un incremento en los tiempos de envío, con el cifrado RSA en un 34% con 90,31 segundos y con el envío en 3DES de un 107% con 139,69 segundos, ambos en comparación con el envío en texto plano.



Figura 29. Resultados de tiempo de carga Host N° 4

La figura N° 30 muestra el envío del archivo desde el host N° 5 de la zona norte 2, con un tiempo de 81,19 segundos en el envío en texto plano, y de 96,65 segundos con el cifrado RSA incrementándose en un 19% y de 130,11 segundos con el cifrado con 3DES incrementándose en un 60%, en relación al primer envío en texto plano.



Figura 30. Resultados de tiempo de carga Host N° 5

Obtenidos los resultados de todos los dispositivos de la zona norte 2, se presentan a continuación en la siguiente tabla N° 8, donde se puede apreciar que se mantiene la tendencia de los dispositivos de la zona anterior, predominando los mejores tiempos en las pruebas con el algoritmo RSA.

Tabla 9. Zona Norte 2.

Host	Variabes	Tiempo de Carga
Host 1	Texto Plano	32,6
	RSA	62,35
	3DES	76,85
Host 2	Texto Plano	40,62
	RSA	72,72
	3DES	130,33
Host 3	Texto Plano	40,83
	RSA	77,9
	3DES	127,79
Host 4	Texto Plano	67,61
	RSA	90,31
	3DES	139,69
Host 5	Texto Plano	81,19
	RSA	96,65
	3DES	130,11

Ficha de recolección de datos N° 2

Se puede considerar en la tabla N° 8 los resultados de la zona Norte 2 que está formada por 5 dispositivos, donde los resultados de las pruebas de tiempo de carga del archivo se muestran tanto en texto plano, cifrados con RSA y cifrado con 3DES, y que son mostrados en el grafico a continuación en la figura 19.

La figura N°31 muestra los valores de la tabla N° 8 en un gráfico de barras, donde están representados los 5 host, cada uno con sus respectivos tiempos de carga del archivo, una tendencia común son los valores de 3DES muy por encima de los valores de RSA.

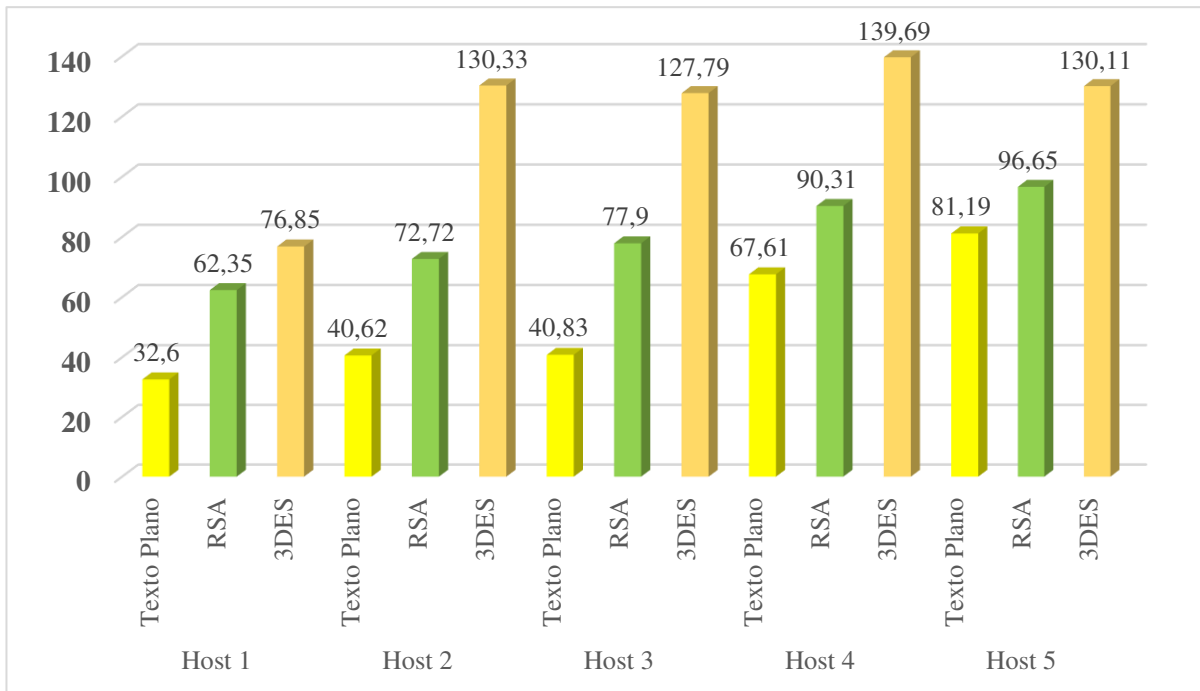


Figura 31. Resumen Tabla N° 9 de Zona Norte 2

3.3.5. Zona Centro 1

Continuando con la presentación de los resultados de las pruebas realizadas por zona, ahora se presentan los resultados de la zona centro 1, y se debe anotar como observación, que está trabajando con un proveedor de internet diferente al de las 2 zonas anteriores.

La figura N° 32 muestra el envío del archivo desde el host N° 1 de la zona centro 1, con un tiempo de envío hasta el repositorio de 3,86 segundos, y en la parte inferior de la figura se muestra el tiempo de 4,91 segundos del cifrado RSA que lo deja con un 27% en el incremento en el tiempo de respuesta, y del cifrado con 3DES con 5,69 segundos, que lo ubica con un 47% de incremento, ambos comparados contra el envío en texto plano.



Figura 32. Resultados de tiempo de carga Host N° 1

La figura N° 33 visualiza el envío del archivo desde el host N° 2 de la zona centro 1, con un tiempo de 3,9 segundos en texto plano, con 4,97 segundos con el cifrado RSA lo que representa un 27% de incremento en el tiempo, y del cifrado con 3DES con 5,44 segundos, lo que representa un 39% de incremento, ambos contra el envío en texto plano.



Figura 33. Resultados de tiempo de carga Host N° 2

La figura N° 34 visualiza el envío del archivo desde el host N° 3 de la zona centro 1, con un tiempo de 3,94 segundos en texto plano, con 4,97 segundos con el cifrado RSA lo que representa un 26% de incremento en el tiempo, y del cifrado con 3DES con 5,48 segundos, lo que representa un 39% de incremento, ambos contra el envío en texto plano.



Figura 34. Resultados de tiempo de carga Host N° 3

La figura N° 35 visualiza el envío del archivo desde el host N° 4 de la zona centro 1, con un tiempo de 3,96 segundos en texto plano, con 4,99 segundos con el cifrado RSA lo que representa un 26% de incremento en el tiempo, y del cifrado con 3DES con 5,47 segundos, lo que representa un 38% de incremento, ambos contra el envío en texto plano.



Figura 35. Resultados de tiempo de carga Host N° 4

La figura N° 36 visualiza el envío del archivo desde el host N° 5 de la zona centro 1, con un tiempo de 4,06 segundos en texto plano, con 5,28 segundos con el cifrado RSA lo que representa un 30% de incremento en el tiempo, y del cifrado con 3DES con 6,52 segundos, lo que representa un 61% de incremento, ambos contra el envío en texto plano.



Figura 36. Resultados de tiempo de carga Host N°5

La figura N° 37 visualiza el envío del archivo desde el host N° 6 de la zona centro 1, con un tiempo de 4,22 segundos en texto plano, con 5,51 segundos con el cifrado RSA lo que representa un 31% de incremento en el tiempo, y del cifrado con 3DES con 5,90 segundos, lo que representa un 40% de incremento, ambos contra el envío en texto plano.



Figura 37. Resultados de tiempo de carga Host N° 6

Los resultados de las pruebas registradas en la zona centro 1 muestran una gran diferencia en tiempos de respuesta en comparación con las zonas anteriores, donde se tiene un proveedor de internet diferente, sin embargo, las diferencias entre los tiempos de envío entre los algoritmos de cifrado, se mantienen.

Tabla 10. Zona Centro 1.

Host	Variables	Tiempo de Carga
Host 1	Texto Plano	3,86
	RSA	4,91
	3DES	5,69
Host 2	Texto Plano	3,9
	RSA	4,97
	3DES	5,44
Host 3	Texto Plano	3,94
	RSA	4,97
	3DES	5,48
Host 4	Texto Plano	3,96
	RSA	4,99
	3DES	5,47
Host 5	Texto Plano	4,06
	RSA	5,28
	3DES	6,52
Host 6	Texto Plano	4,22
	RSA	5,51
	3DES	5,9

En la tabla N° 9 se presentan los resultados de las pruebas tomadas en la zona centro 1, con 6 hosts, se puede visualizar una mejora en tiempos de respuesta, pero el porcentaje de diferencia entre los tiempos de respuesta entre los mecanismos de cifrado se mantiene.

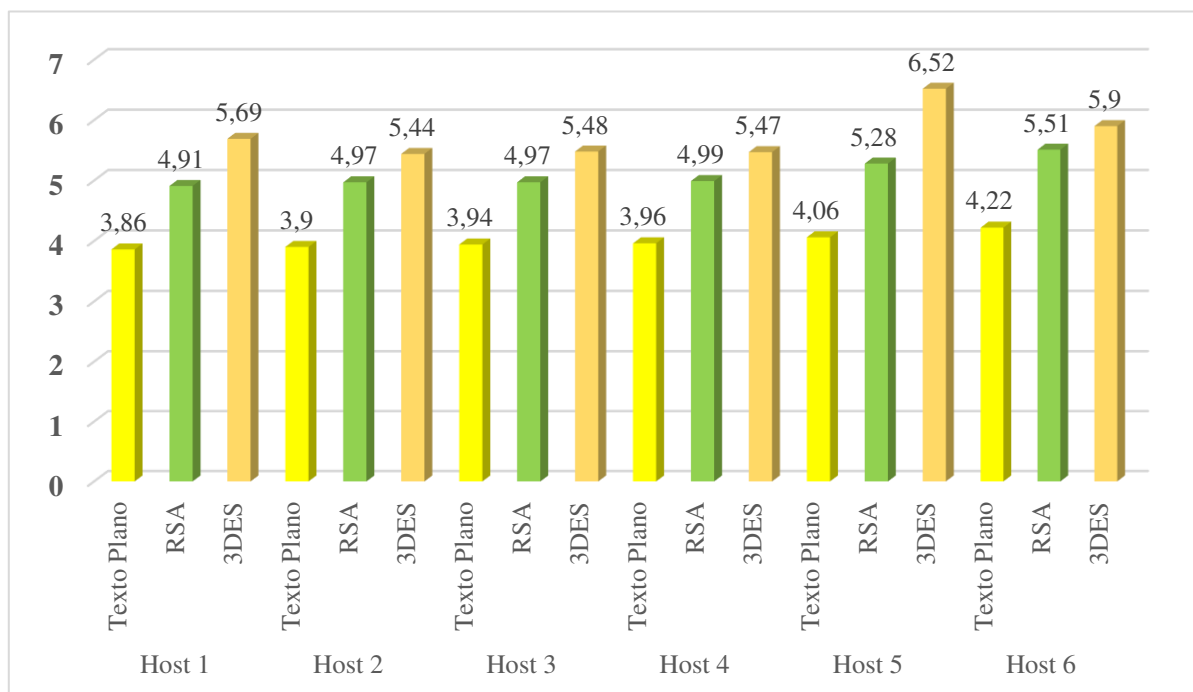


Figura 38. Resumen Tabla N° 10 de Zona Centro 1

De igual manera en la figura N° 38 se presentan de una manera gráfica los resultados de la zona centro 1, donde se refleja que RSA sigue siendo más rápido en cuanto al envío del archivo cifrado.

3.3.6. Zona Centro 2

La figura N° 39 muestra el envío del archivo desde el host N° 1 de la zona centro 2, con un tiempo de envío hasta el repositorio de 5,11 segundos, y en la parte inferior de la figura se muestra el tiempo de 5,71 segundos del cifrado RSA que lo deja con un 12% en el incremento en el tiempo de respuesta, y del cifrado con 3DES con 6,05 segundos, que lo ubica con un 18% de incremento, ambos comparados contra el envío en texto plano.



Figura 39. Resultados de tiempo de carga Host N° 1

La figura N° 40 muestra el envío del archivo desde el host N° 2 de la zona centro 2, con un tiempo de envío hasta el repositorio de 5,52 segundos, y en la parte inferior de la figura se muestra el tiempo de 5,74 segundos del cifrado RSA que lo deja con un 4% en el incremento en el tiempo de respuesta, y del cifrado con 3DES con 6,93 segundos, que lo ubica con un 26% de incremento, ambos comparados contra el envío en texto plano.



Figura 40. Resultados de tiempo de carga Host N° 2

La figura N° 41 muestra el envío del archivo desde el host N° 3 de la zona centro 2, con un tiempo de envío hasta el repositorio de 7,07 segundos, y en la parte inferior de la figura se muestra el tiempo de 7,18 segundos del cifrado RSA que lo deja con un 2% en el incremento en el tiempo de respuesta, y del cifrado con 3DES con 10,39 segundos, que lo ubica con un 47% de incremento, ambos comparados contra el envío en texto plano.



Figura 41. Resultados de tiempo de carga Host N° 3

La figura N° 42 muestra el envío del archivo desde el host N° 4 de la zona centro 2, con un tiempo de envío hasta el repositorio de 7,16 segundos, y en la parte inferior de la figura se muestra el tiempo de 7,52 segundos del cifrado RSA que lo deja con un 5% en el incremento en el tiempo de respuesta, y del cifrado con 3DES con 8,57 segundos, que lo ubica con un 20% de incremento, ambos comparados contra el envío en texto plano.



Figura 42. Resultados de tiempo de carga Host N° 4

La figura N° 43 muestra el envío del archivo desde el host N° 5 de la zona centro 2, con un tiempo de envío hasta el repositorio de 7,45 segundos, y en la parte inferior de la figura se muestra el tiempo de 9,52 segundos del cifrado RSA que lo deja con un 28% en el incremento en el tiempo de respuesta, y del cifrado con 3DES con 10,62 segundos, que lo ubica con un 43% de incremento, ambos comparados contra el envío en texto plano.



Figura 43. Resultados de tiempo de carga Host N° 5

La figura N° 44 muestra el envío del archivo desde el host N° 6 de la zona centro 2, con un tiempo de envío hasta el repositorio de 9,32 segundos, y en la parte inferior de la figura se muestra el tiempo de 9,59 segundos del cifrado RSA que lo deja con un 15% en el incremento en el tiempo de respuesta, y del cifrado con 3DES con 10,43 segundos, que lo ubica con un 25% de incremento, ambos comparados contra el envío en texto plano.



Figura 44. Resultados de tiempo de carga Host N° 6

A continuación se muestra la tabla N° 10 con el resumen de los resultados de las pruebas realizadas en la zona centro 2, donde se puede comprobar una concordancia con los resultados obtenidos en la zona centro 1, a cargo del mismo proveedor de internet.

Tabla 11. Zona Centro 2.

Host	Variables	Tiempo de Carga
	Texto Plano	5,11
Host 1	RSA	5,71
	3DES	6,05
	Texto Plano	5,52
Host 2	RSA	5,74
	3DES	6,93
	Texto Plano	7,07
Host 3	RSA	7,18
	3DES	10,39
	Texto Plano	7,16
Host 4	RSA	7,52
	3DES	8,57
	Texto Plano	7,45
Host 5	RSA	9,52
	3DES	10,62
	Texto Plano	8,32
Host 6	RSA	9,59
	3DES	10,43

Ficha de recolección de datos N° 3

Como queda demostrado en la tabla N° 10, los porcentajes en tiempos de envío siguen manteniéndose, dejando ver que RSA es más rápido en cuanto al proceso de cifrado y envío del documento hasta el repositorio central.

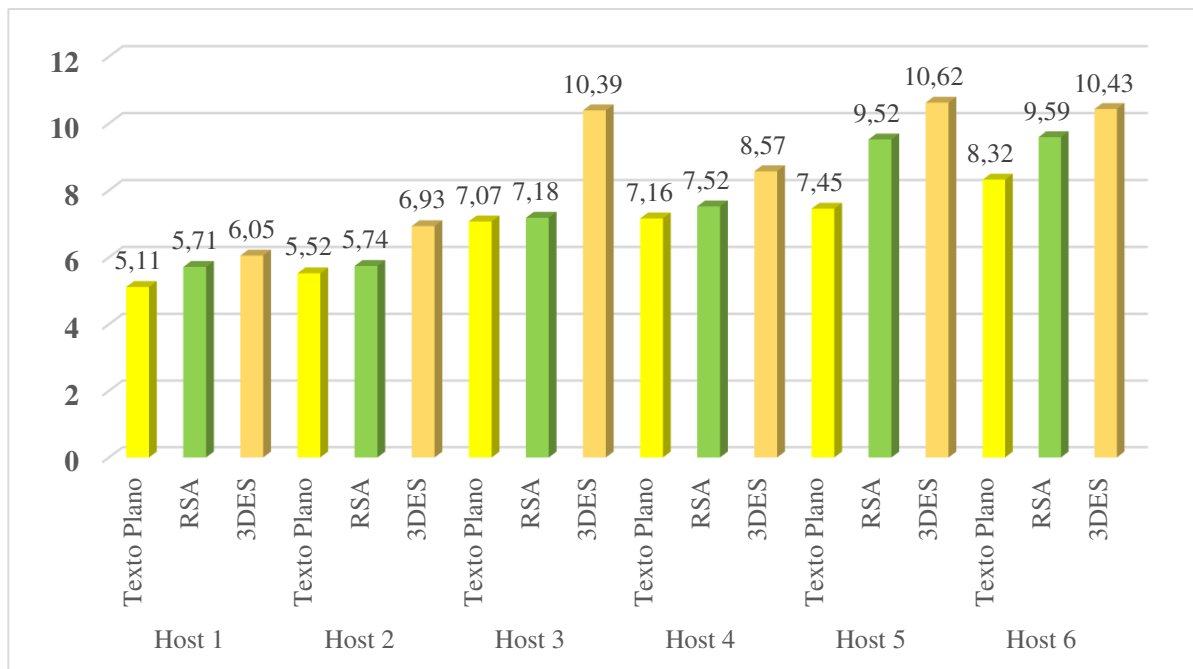


Figura 45. Resumen Tabla N° 11 de Zona Norte 2

De manera gráfica, en la figura N°45 se presentan los resultados obtenidos en la zona centro 2, confirmando a RSA como más rápido en entregar al repositorio la información cifrada, hasta el momento.

3.3.7. Zona Sur 1

Las zonas sur 1 y 2 son las zonas con menor número de haciendas, y comparten el mismo proveedor de internet de las zonas centro1 y 2. La figura N° 46 muestra el envío del archivo desde el host N° 1 de la zona sur 1, con un tiempo de envío hasta el repositorio de 3,48 segundos, y en la parte inferior de la figura se muestra el tiempo de 4,10 segundos del cifrado RSA que lo deja con un 18% en el incremento en el tiempo de respuesta, y del cifrado con 3DES con 4,62 segundos, que lo ubica con un 33% de incremento, ambos comparados contra el envío en texto plano.



Figura 46. Resultados de tiempo de carga Host N° 1

La figura N° 47 muestra el envío del archivo desde el host N° 2 de la zona sur 1, con un tiempo de envío hasta el repositorio de 3,56 segundos, y en la parte inferior de la figura se muestra el tiempo de 4,36 segundos del cifrado RSA que lo deja con un 22% en el incremento en el tiempo de respuesta, y del cifrado con 3DES con 5,13 segundos, que lo ubica con un 44% de incremento, ambos comparados contra el envío en texto plano.



Figura 47. Resultados de tiempo de carga Host N° 2

La figura N° 48 muestra el envío del archivo desde el host N° 3 de la zona sur 1, con un tiempo de envío hasta el repositorio de 3,85 segundos, y en la parte inferior de la figura se muestra el tiempo de 4,72 segundos del cifrado RSA que lo deja con un 23% en el incremento en el tiempo de respuesta, y del cifrado con 3DES con 5,21 segundos, que lo ubica con un 35% de incremento, ambos comparados contra el envío en texto plano.



Figura 48. Resultados de tiempo de carga Host N° 3

En la tabla N° 11 se muestran los resultados de las pruebas realizadas en la zona sur 1, coincidiendo con los resultados de las zonas anteriores, manteniendo tiempos de envío mucho menores que las zonas norte 1 y 2, pero sosteniendo la brecha entre los algoritmos RSA y 3DES.

Tabla 12. Zona Sur 1

Host	Variables	Tiempo de Carga
Host 1	Texto Plano	3,48
	RSA	4,1
	3DES	4,62
Host 2	Texto Plano	3,56
	RSA	4,36
	3DES	5,13
Host 3	Texto Plano	3,85
	RSA	4,72
	3DES	5,21

Ficha de recolección de datos N° 4

Finalmente en la figura 49, se muestra el resumen de los datos de la zona sur 1 de manera gráfica, permitiendo comprender mejor las diferencias de tiempos entre los diferentes formatos de envíos.

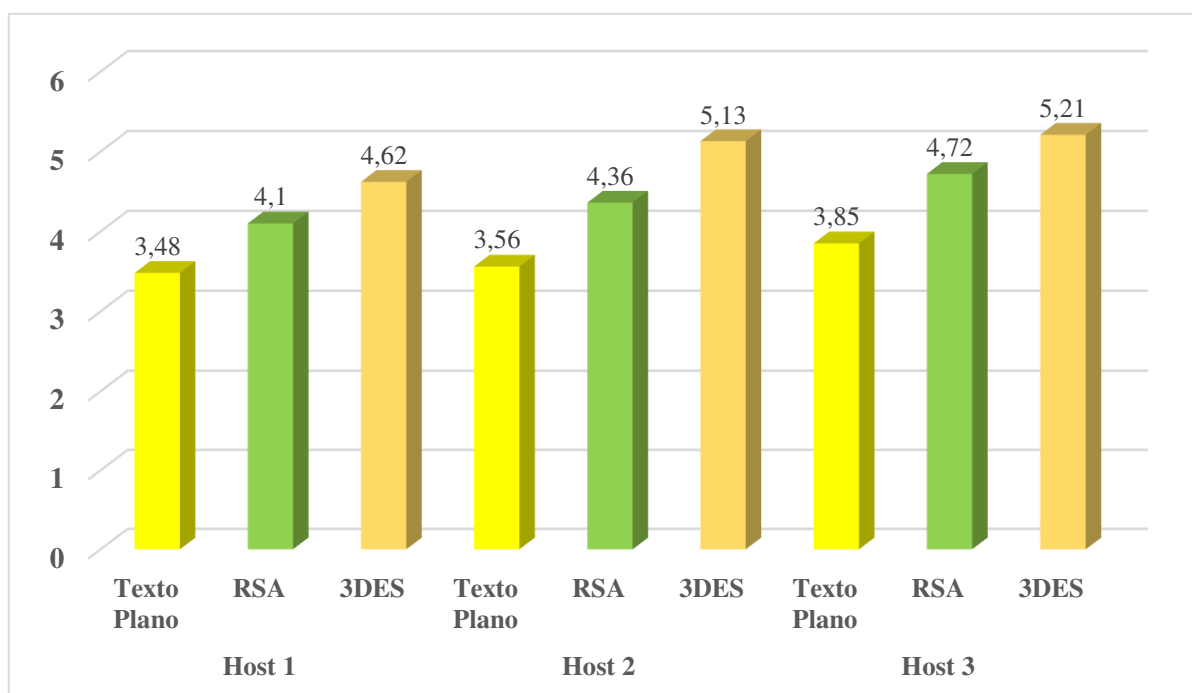


Figura 49. Resumen Tabla N° 12 de Zona Sur 1

3.3.8. Zona Sur 2

La figura N° 50 muestra el envío del archivo del único host de la zona, con un tiempo de envío hasta el repositorio de 8,60 segundos, y en la parte inferior de la figura se muestra el tiempo de 15,75 segundos del cifrado RSA que lo deja con un 83% en el incremento en el tiempo de respuesta, y del cifrado con 3DES con 16,03 segundos, que lo ubica con un 86% de incremento, ambos comparados contra el envío en texto plano.



Figura 50. Resultados de tiempo de carga Host N°1

En la tabla N° 12 se muestra el resultado tomado del único host de prueba de la zona sur 2, presentando datos parecidos a los obtenidos anteriormente.

Tabla 13. Zona Sur 2.

Host	Variables	Tiempo de Carga
Host 1	Texto Plano	8,6
	RSA	15,75
	3DES	16,03

Ficha de recolección de datos N° 5

En la figura N° 52 se muestra gráficamente los resultados presentados en la tabla N° 12, dejando ver una vez más en claro que el algoritmo RSA demuestra ser el mecanismo de cifrado con mejor tiempo de respuesta en el proceso de envío de la información.

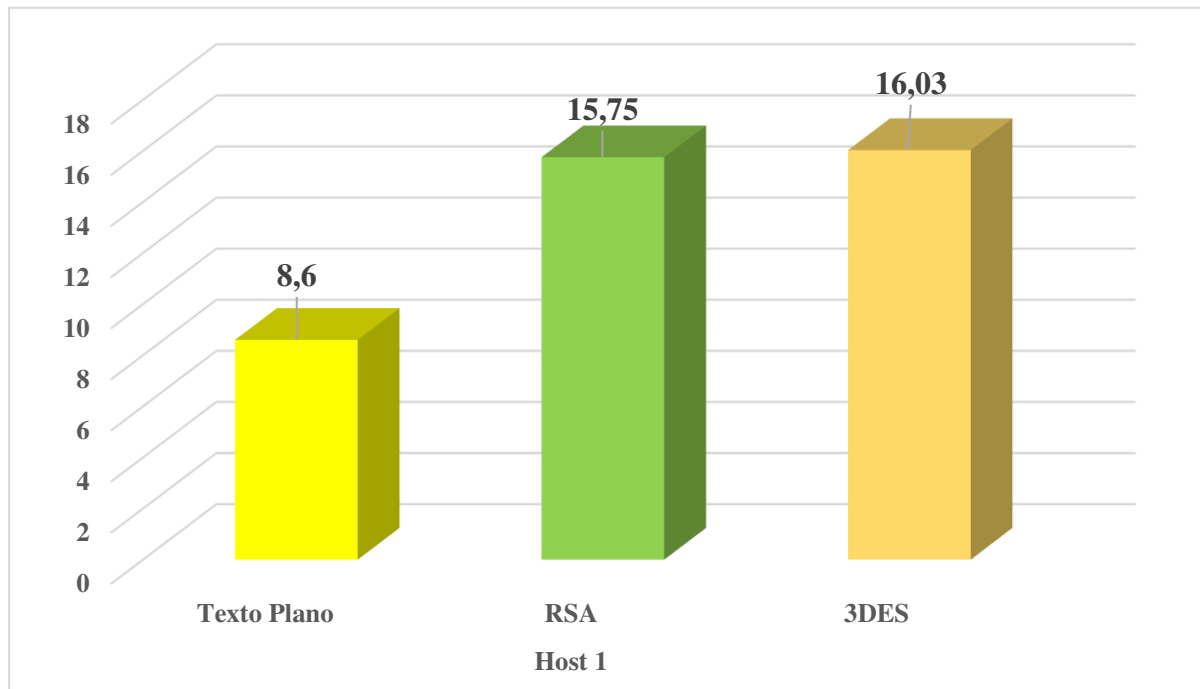


Figura 52. Resumen Tabla N° 13 de Zona Sur 2

3.3.9. Resumen de tiempos de carga al repositorio

Durante el proceso de levantamiento de la información, resultado de las pruebas realizadas en los diferentes dispositivos de las 6 zonas, se ha logrado notar que en las zonas norte 1 y 2 que están con el proveedor de internet número 1, los tiempos de entrega de la información son mucho más altos que los tiempos de respuesta de las zonas centro 1 y 2 y sur 1 y 2, que están con el proveedor de internet número 2.

En la tabla N° 13 se ha realizado un resumen promediando los resultados de todas las zonas en las que se han realizado las pruebas de tiempos de envío del archivo cifrado con los datos de las labores del proceso diario de las respectivas haciendas.

Tabla 14. Resumido de Tiempos de Carga del archivo al Repositorio.

Archivo	Variables	Tamaño del Archivo
	Texto Plano	18,6
Archivo	RSA	29,4
	3DES	47,8

Promedio general de las 6 zonas.

El promedio de todos los resultados obtenidos durante el proceso de pruebas, representado por la figura N° 53, demuestra que, el cifrado con el algoritmo RSA se presenta con 29,4 segundos, mientras que 3DES se presenta con 47,8, lo que, en comparación con el promedio del tiempo de envío del archivo en texto plano que es 18,6 segundos, deja como resultado lo siguiente:

- El algoritmo RSA incremento el tiempo de respuesta durante el envío del archivo cifrado desde los dispositivos Raspberry hasta el repositorio central en un 58%.
- El algoritmo 3DES incremento el tiempo de respuesta durante el envío del archivo cifrado desde los dispositivos Raspberry hasta el repositorio central en un 157%.

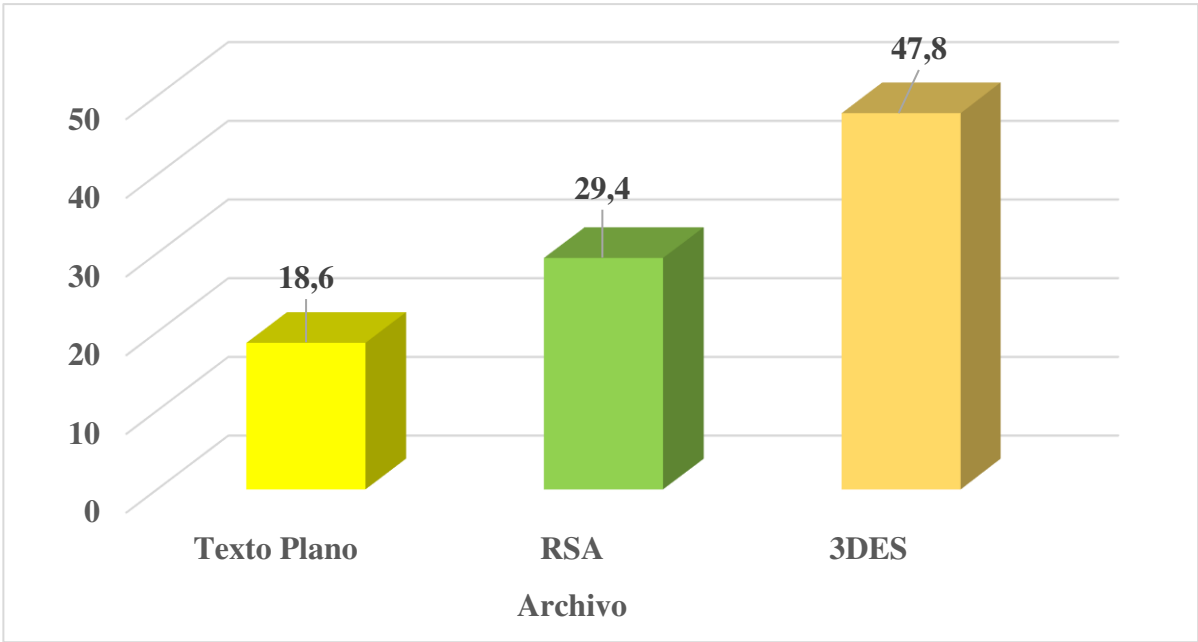


Figura 53. Resumen Tabla N° 14 de Tiempos de Carga de Archivo

4. Conclusiones

Luego del análisis de la información obtenida durante la investigación, se puede concluir lo siguiente:

En Internet existen muchos sitios, ya sea en bibliotecas en línea, foros de investigación, y en muchos otros portales de interés científico, donde se encuentra información sobre investigaciones realizadas, y se compara variados algoritmos de encriptación, en los que se mide no solo la velocidad de proceso, sino también vulnerabilidad del cifrado, e incluso la capacidad de resistir los ataques de diversos programas para romper la seguridad del cifrado, y siempre se lo hace en equipos computacionales robustos con memorias de hasta 32 Gb de memoria RAM y con procesadores de última generación, sin embargo, estas mismas investigaciones no se las ha realizado en dispositivos con recursos limitados como lo son los dispositivos de placa única Raspberry Pi o Arduino.

En las pruebas realizadas a los 25 hosts, evidencia que el algoritmo asimétrico de cifrado RSA, variante ultima a la fecha de la realización de esta investigación, supera en un 100% con 29,4 segundos al cifrado con el algoritmo 3DES, que tardó 47,8 segundos, con respecto al tiempo de proceso de cifrado del archivo en texto plano que contiene la información del proceso diario de las haciendas donde se realizaron las pruebas, comparados ambos con el envío del archivo en texto plano que tardó 18,6 segundos en entregarse en el repositorio central de la empresa.

Es importante aclarar que, en el tiempo de carga del archivo se tiene que considerar el tiempo que tarda el algoritmo en efectuar el proceso de cifrado, lo que demuestra que el algoritmo RSA es más rápido en cuanto a este proceso que el algoritmo 3DES.

Además de haber obtenido un mejor tiempo durante el envío, RSA también logró un tamaño del archivo cifrado menor que 3DES, es decir, RSA se incrementó en un 167% con 1,5 Mb, mientras que 3DES se incrementó en un 300% su tamaño con 2,2 Mb, ambos en relación al tamaño del archivo en texto plano que pesaba 0,571 Mb.

Otro punto importante que se debe anotar es que, el algoritmo 3DES utiliza claves de 112 bits de longitud, mientras que RSA utiliza claves de al menos 1024 bits, lo que deja claro que es más robusto en cuanto a seguridad.

Sin embargo, pese a la información obtenida en esta investigación, se debe aclarar que en cualquier caso, será la gerencia del área de TI quien finalmente decida sobre tal o cual sistema de cifrado aplicar para el área de trabajo.

5. Recomendaciones

En cuanto a las recomendaciones, son varios los puntos considerados como meritorios a ser nombrados en la siguiente lista, así se tienen los siguientes:

Realizar las pruebas en otras plataformas como dispositivos HummingBoard, que presenta características de hardware similares a Raspberry Pi, igualmente BeagleBone Black y Odroid U3 que llega a alcanzar las 2 GB de memoria RAM, para confirmar los resultados, siendo estos también microordenadores de placa única, los resultados podrían contrastarse con los obtenidos en la presente investigación.

Con el fin de alcanzar un mayor grado de seguridad, incorporar otros algoritmos de cifrado como AES y combinarlos con los utilizados en la presente investigación y comparar los resultados.

Utilizar otros tipos de archivos de mayor tamaño durante el proceso de pruebas, como imágenes, pdf, audios y videos, que tengan tamaños superiores a los utilizados en la presente investigación.

Por todo lo anteriormente expuesto, se puede concluir que RSA es el algoritmo con menos tiempo de respuesta durante el proceso de envío y menor tamaño en el crecimiento del archivo durante el cifrado.

6. Bibliografía

- Alegre Ramos, M. (2010). *Sistemas Operativos Monopuesto*. Madrid, Madrid, España: Paraninfo. Recuperado el 30 de Octubre de 2018
- Algaba, P., Martín, A., & Lechuga, P. (2017). *La implantación de un sistema ERP para la gestión de la información*. Cadiz, Andalucía, España: Eumed.
- Ander-Egg, E. (1995). Técnicas de investigación social. En E. Ander-Egg, *Técnicas de investigación social* (pág. 423). Buenos Aires: Lumen.
- Ariansen, R., & Rojas, J. (2017). *Implementación de Protocolo de Cifrado TLS para mejorar la Seguridad de la capa de Transporte*. Chiclayo, Chiclayo, Peru: Universidad Señor de Sipan. Recuperado el 25 de Septiembre de 2018
- Caballero, C., & Clavero, J. A. (2017). *UF1473 - Salvaguarda y seguridad de los datos*. Madrid, Madrid, España: Ediciones Paraninfo, S.A.
- Camazón, J. (2011). *Sistemas operativos monopuesto*. (Editex, Ed.) Madrid, Madrid, España: Editex. Recuperado el 2 de Noviembre de 2018
- Cazau, P. (2006). *Introducción a la investigación en ciencias sociales*. Buenos Aires.
- Cisco Systems, Inc. (1 de Noviembre de 2018). *www.cisco.com*. Obtenido de <https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html>
<https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html>
- Commons, Licencia Creative. (10 de Noviembre de 2018). https://es.wikipedia.org/wiki/Categor%C3%ADa:Wikipedia:Derechos_de_autor. Obtenido de <https://es.wikipedia.org/wiki/Wikipedia:Portada>: https://es.wikipedia.org/wiki/Placa_computadora
- Cortes, D., & Ardila, A. (2012). *Metodología para la implementación de un sistema integrado de gestión con las normas ISO 9001, ISO 20000 e ISO 27001*. Bogota: UNIVERSIDAD EAN.
- Creative Commons Attribution ShareAlike 3.0. (3 de Noviembre de 2018). www.arduino.cc/en/Guide/Introduction. Obtenido de www.arduino.cc/en/Main/AboutUs: <https://www.arduino.cc/en/Guide/Introduction#>
- Gil Pascual, J. (2016). *TÉCNICAS E INSTRUMENTOS PARA LA RECOGIDA DE INFORMACIÓN*. Madrid: UNED.
- González, K., & Urrego, G. (01 de Diciembre de 2014). Estudio sobre Computadores de Placa Reducida Raspberry Pi Modelo B y Cubieboard2. *ENGI Revista Electrónica de la Facultad de Ingeniería*, 5. Obtenido de

- http://revistas_electronicas.unicundi.edu.co/index.php/Revistas_electronicas/informacion/librarians
- Goñi, I. (01 de 01 de 2005). <http://www.scielo.org/php/index.php?lang=es>. Recuperado el 30 de Agosto de 2018, de http://www.scielo.org: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352000000300005#x
- Granados Paredes, G. (10 de Julio de 2006). Introducción a la Criptografía. *Revista Digital Universitaria*, 17. Recuperado el 30 de agosto de 2018, de <http://www.revista.unam.mx/vol.7/num7/art55/int55.htm>
- Guaña Mora, E. J. (2016). *Diseño de una red de sensores inalambricos para monitorear parametros relacionados con la agricultura*. Quito: UPL.
- iso. (20 de Septiembre de 2018). www.iso27000.es. Obtenido de <http://www.iso27000.es/iso27000.html>
- Jean-Francois, C. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas*. Barcelona, España: Ediciones ENI. Recuperado el 29 de Agosto de 2018
- Jiménez, T. (2015). *Gestión de recursos, servicios y de la red de comunicaciones*. Madrid, España: Elearning, S.L.
- López Neira, A., & Ruiz Spohr, J. (01 de 01 de 2012). <http://www.iso27000.es>. Recuperado el 30 de Agosto de 2018, de <http://www.iso27000.es/iso27000.html: http://www.iso27000.es/iso27000.html>
- Muñoz, J. (2017). *Diseño de un plan estratégico para la seguridad de la información de CIAS & Profesionales S.A.S*. San Miguel de Agreda de Mocoa, Putumayo, Colombia. Obtenido de <http://hdl.handle.net/10596/14448>
- Plaza, J., Mendo, A., & Sánchez, V. (2006). Sistema de codificación y análisis de la calidad del dato en el tenis de dobles. *Revista de psicología del deporte*, 279-294.
- Ramirez Morales, I., & Mazon Olivo, B. (2017). *Análisis de Datos Agropecuarios* (2018 ed.). Machala, El Oro, Ecuador: UTMACH. Recuperado el 29 de Agosto de 2018
- Rosñol Ruiz, P. (2015). *Verificación y resolución de incidencias en una red de área local*. Madrid, Madrid, España: Editorial Elearning. Recuperado el 20 de Octubre de 2018
- Software in the Public Interest, Inc. (25 de Julio de 2018). <https://www.debian.org>. Recuperado el 3 de Septiembre de 2018, de Debian: <https://www.debian.org/intro/about>
- Tanenbaum, A. S. (2003). *Redes de computadoras*. Mexico, Mexico, Mexico: Pearson Educación.

USERSHOP. (2015). *Redes avanzadas*. España: USERSHOP.

USERSHOP. (2015). *Redes avanzadas*. España: USERSHOP.

Yacuzzi, E. (2004). El diseño experimental y los métodos de Taguchi: Conceptos y aplicaciones en la industria farmacéutica. (U. o. CEMA, Ed.) *UCEMA*, 32. Recuperado el 22 de Octubre de 2018

7. Anexos

7.1. Anexo 1. Ficha de Observación

Ficha de recolección de Datos				
Pruebas de velocidad de carga de archivo hasta el Repositorio				
Zona	Host	Tiempo de Carga		
		Texto Plano	RSA	3DES
ZONA NORTE 1	1	26,94	54,44	80,33
	2	28,79	57,05	132,88
	3	31,37	57,90	136,98
	4	31,47	61,03	121,69
ZONA NORTE 2	5	32,60	62,35	76,85
	6	40,62	72,72	130,33
	7	40,83	77,90	127,79
	8	67,61	90,31	139,69
	9	81,19	96,65	130,11
ZONA CENTRO 1	10	3,86	4,91	5,69
	11	3,90	4,97	5,44
	12	3,94	4,97	5,48
	13	3,96	4,99	5,47
	14	4,06	5,28	6,52
	15	4,22	5,51	5,90
ZONA CENTRO 2	16	5,11	5,71	6,05
	17	5,52	5,74	6,93
	18	7,07	7,18	10,39
	19	7,16	7,52	8,57
	20	7,45	9,52	10,62
	21	8,32	9,59	10,43
ZONA SUR 1	22	3,48	4,10	4,62
	23	3,56	4,36	5,13
	24	3,85	4,72	5,21
ZONA SUR 2	25	8,60	15,75	16,03
Observaciones:				

7.2. Anexo 2. Políticas de Seguridad

Política de Protección de llaves/claves de cifrado

Diciembre 2018

1. Introducción

La administración de llaves/claves para cifrado, si no se hace correctamente, puede conducir al compromiso y divulgación de las llaves/claves privadas que se utilizan para proteger los datos sensibles y por tanto el compromiso de los datos. Es posible que los usuarios entiendan la importancia del cifrado de ciertos documentos y de las comunicaciones electrónicas, pero pudieran no estar familiarizados con las reglas mínimas para la protección de las llaves/claves de cifrado.

Nota: Cuando nos refiramos a tecnología PKI utilizaremos la palabra “Llave” y cuando nos refiramos a una contraseña para cifrado simétrico utilizaremos la palabra “Clave” y cuando no refiramos a las dos tecnologías usaremos llaves/claves como las traducciones más apropiadas del inglés al español de la palabra “key”.

2. Objetivo

Esta política describe los requisitos para proteger las llaves/claves de cifrado que se encuentran bajo el control de los usuarios finales. Estos requisitos están diseñados para evitar la divulgación no autorizada y su posible uso fraudulento posterior. Los métodos de protección previstos incluirán controles operacionales y técnicos, tales como procedimientos de copias de seguridad, cifrado bajo una llaves/claves distinta y el uso de hardware reforzado en seguridad.

3. Alcance

Esta política aplica a cualquier llaves/claves de cifrado listada a continuación y a cualquier persona responsable de alguna de estas llaves/claves de cifrado. Las llaves/claves de cifrado cubiertas por esta política son:

- Llaves/claves de cifrado emitidas por la empresa
- Llaves/claves de cifrado utilizadas para negocios de la empresa
- Llaves/claves de cifrado utilizadas para proteger datos propiedad de la empresa

Las llaves públicas contenidas en los certificados digitales están explícitamente exentas de esta política

4. Política

Todas las llaves/claves de cifrado cubiertas por esta política deben ser protegidas para evitar su divulgación no autorizada y su posible uso fraudulento posterior.

4.1 Claves secretas para cifrado simétrico

Las claves secretas utilizadas para cifrado simétrico, también llamada criptografía de clave simétrica, deben de estar protegidas mientras se distribuyen a todas las partes que las van a utilizar.

Durante la distribución de claves secretas se debe de utilizar cifrado simétrico, las claves de cifrado simétrico para envío deben de utilizar el algoritmo más fuerte especificado en la política de cifrado aceptable de la empresa, con la clave de la longitud más larga permitida.

Si las claves de cifrado simétrico son para cifrar un algoritmo más fuerte, entonces las claves para envío deben de dividirse, cada parte de la clave de cifrado a enviar con una clave de cifrado simétrico diferente que sea de la longitud de clave más larga autorizada y después cada porción cifrada se transmite utilizando diferentes mecanismos de transmisión. El objetivo es proporcionar la protección más rigurosa a la clave en el envío que a los datos que se cifraran con esa clave de cifrado. Las claves para cifrado simétrico, cuando están en reposo, deben de estar protegidas con medidas de seguridad al menos tan estrictas como las medidas utilizadas para la distribución de esa clave.

4.2 Llaves de cifrado de PKI

La criptografía de llave pública o la criptografía asimétrica, utiliza pares de llaves públicas y privadas. La llave pública se pasa a la autoridad de certificación para ser incluida en el certificado digital emitido para el usuario final. El certificado digital está disponible para todo el mundo una vez emitido. La llave privada sólo debe estar disponible para el usuario final al que se expide el certificado digital correspondiente.

4.2.1 Infraestructura de llave pública (PKI) de la empresa

Los pares de llaves pública y privada emitidas por la infraestructura de llave pública (PKI) de la empresa se generan en Smart Cards reforzadas emitidas a un usuario final específico. La llave privada asociada con el certificado de identidad de un usuario final, que sólo se utiliza para las firmas digitales, nunca deberá de salir de la Smart Card, esto evita que el equipo de TecnoSegIsrael guarde la llave en el depósito en garantía cualquier llave privada relacionadas con los certificados de identidad. La llave privada asociada con algún certificado de cifrado, que se utiliza para cifrar correo electrónico y otros documentos, debe de estar custodiada en el depósito en garantía en cumplimiento de las políticas de la empresa.

El acceso a las llaves privadas almacenadas en una Smart Card emitida por la empresa estará protegido por un número de identificación personal (PIN) que sólo es conocida por el individuo a quien se emite la Smart Card. El software de la Smart Card será configurado para requerir la introducción del PIN antes acceder a cualquier llave privada contenida en la Smart Card que se está accediendo.

4.2.2 Otras llaves de cifrado de PKI

Otros tipos de llaves pueden ser generadas en software en la computadora del usuario final y pueden ser almacenados como archivos en el disco duro o en un Token de hardware. Si las llaves son generadas en software, se requiere que el usuario final realice al menos una copia de seguridad de estas llaves y almacene cualquier copia de seguridad de manera segura. También se requiere que el usuario cree una copia en el depósito en garantía (Scrow) de cualquier llave privada utilizada para cifrado de datos y

entregue una copia al representante local de seguridad de la información para su almacenamiento seguro.

El equipo de TecnoSegIsrael no guardará en depósito en garantía (escrow) ninguna llave privadas relacionadas con certificados de identidad. Todas las copias de seguridad, incluidas las copias de depósito en garantía (escrow), deberán de estar protegidas con una contraseña o passphrase que cumpla con la Política de Contraseñas de la Empresa. Los representantes de TecnoSegIsrael guardarán y protegerán las llaves en el depósito de garantía (escrow) como se describe en la Política de Declaración de la Práctica de Certificados.

4.3 Números de Identificación Personal (PIN), Contraseñas y Pass frases

Todos los PINs, contraseñas o pass frases utilizadas para proteger las llaves de cifrado deben cumplir con los requisitos de complejidad y longitud descritos en la Política de Contraseñas de la Empresa.

4.4 Pérdida y Robo

La pérdida, robo o posible divulgación no autorizada de cualquier llave/clave de cifrado cubierto por esta política debe de ser reportado inmediatamente al equipo TecnoSegIsrael. El personal de TecnoSegIsrael apoyará al usuario final con cualquier acción necesaria en relación con la revocación de los certificados o los pares de llaves públicas y privadas o el cambio de clave en caso de cifrado simétrico.

5. Cumplimiento de la política

5.1 Medidas de Cumplimiento.

El equipo TecnoSegIsrael verificará el cumplimiento de esta política a través de diversos métodos, incluyendo pero no limitado a periódica revisiones periódicas caminando (walk- thru), video vigilancia, informes de herramientas de negocio, auditorías internas y externas y retroalimentación al dueño de la política.

5.2 Excepciones

Cualquier excepción a la norma debe ser aprobada por el equipo de TecnoSegIsrael con antelación.

5.3 Incumplimiento

Un empleado que se encuentre que haya violado esta política puede estar sujeto a medidas disciplinarias, hasta e incluyendo la terminación del empleo.

6. Procesos y estándares relacionados.

- Política de cifrado Aceptable
- Política de Declaración de Prácticas de Certificados
- Política de Contraseñas
- Política de Seguridad Física

7. Temimos y definiciones

Los siguientes términos y definición se pueden encontrar en el Glosario de Cero Uno Software situado en: <https://www.cerounosoftware.com/security-resources/glossary-of-terms/>

- Autoridad Certificadora (CA)
- Certificado Digital
- Firma digital
- Texto plano
- Criptografía de llave pública
- Pares de llave pública
- Criptografía simétrica

8. Historial de Revisión

<i>Fecha de Cambio</i>	<i>Responsable</i>	<i>Resumen de cambios</i>
<i>Diciembre 2018</i>	Equipo de Políticas de Seguridad de Software	Creación

ANÁLISIS DE TECNOLOGÍAS CRIPTOGRÁFICAS EN PLATAFORMAS CON MICROORDENADORES DE PLACA ÚNICA

Autores: Gregorio Aurelio Camacho Reina
e-mail: camachoarelio@gmail.com
Edison Javier Guaña Moya
e-mail: edisonjavier02@gmail.com

RESUMEN: Con los avances en las tecnologías de la información, cada vez son más los procesos que son automatizados, consecuentemente, la información que se genera va cada vez en aumento. La centralización de la información se convierte en una necesidad, por lo que las empresas se ven obligadas a enviar desde sus sucursales toda esta información a un repositorio central.

El transporte de la información por toda la red debe realizarse de una manera segura y rápida, siendo necesario utilizar mecanismos que apoyen este primer factor, y uno de ellos es la criptografía.

El presente trabajo describe las particularidades de los diversos sistemas de encriptación y su rendimiento en plataformas, con características de hardware reducidas.

Como resultado se constata que el algoritmo asimétrico de cifrado RC4 supera en este entorno al algoritmo 3DES.

PALABRAS CLAVE: Cifrado, Criptografía, ISO 27001, Raspberry.

ABSTRACT. With the advances in information technologies, more and more processes are automated, consequently, the information that is generated is increasing every time. The centralization of information becomes a necessity, so companies are forced to send all this information from their branches to a central repository.

The transport of information throughout the network must be done in a safe and fast way, being necessary to use mechanisms that support this first factor, and one of them is cryptography.

The present work describes the particularities of the various encryption systems and their performance on platforms, with reduced hardware characteristics.

As a result, it is found that the asymmetric encryption algorithm RC4 exceeds in this environment the 3DES algorithm.

Keywords: Encryption, Cryptography, ISO 27001, Raspberry.

1 INTRODUCCIÓN

En la actualidad, el avance tecnológico está llegando a todas las áreas de todo tipo de negocio y la agricultura no ha sido la excepción. En empresas agrícolas del Ecuador, utilizan un Sistema de Balanzas Electrónicas (SBE) que es una aplicación web, mediante la cual se registran datos del proceso de embalaje de frutas en sus estaciones de trabajo. Esta información recolectada diariamente en la aplicación cliente es migrada a repositorios que en muchas ocasiones se encuentran ubicados en otras ciudades; por lo que es muy importante que ésta llegue de una forma rápida y segura.

Por esto, la empresa necesitaría un mecanismo de cifrado que asegure la transmisión y recepción de la información, y que su contenido esté protegido, pero a la vez, sin provocar un colapso de la intranet, induciendo a los demás usuarios de la red al retraso en sus labores. De aquí que sea muy importante elegir el mecanismo de seguridad adecuado que mantenga el equilibrio perfecto entre seguridad y manejo de datos.

Son muchos los métodos de seguridad aplicables, uno de ellos es la encriptación de datos, existe mucha información en la red sobre las características, ventajas y desventajas de cada uno de los diferentes mecanismos de encriptación, implementados en equipos computacionales con características robustas y los resultados son muy satisfactorios.

En la actualidad existe una amplia variedad de sistemas criptográficos, y saber elegir la herramienta adecuada exige un análisis exhaustivo de sus características conociendo su clasificación y conceptos fundamentales, para poder darle un uso adecuado y sacar el mayor beneficio posible.

Generalmente los dispositivos Raspberry se han utilizado para desarrollo a nivel didáctico por la facilidad de adquisición y mantenimiento, pero en la actualidad se está implementando este tipo de equipos en proyectos en empresas agrícolas (González & Urrego, 2014).

En sí mismo cada mecanismo de cifrado posee un funcionamiento diferente al de los demás, lo que supone cargas de trabajo diferentes. Los dispositivos Raspberry aún en su versión más actual cuentan con características de procesamiento que limita sus funciones, por lo que es necesario realizar pruebas en sus

ambientes más extremos para considerarlos idóneos antes de su lanzamiento a producción.

Es por ello que, en la presente investigación se realizarán pruebas de cifrado con 2 algoritmos, cada uno con estructuras diferentes, en equipos de Raspberry Pi2. Se identificarán las particularidades de los diversos sistemas de encriptación y su rendimiento en plataformas, con características de hardware reducidas, llegando a alcanzar armonía entre carga de proceso y tiempos de respuesta.

2 TEORÍA Y CONTEXTO

2.1 Algoritmos de cifrado

La llegada y desarrollo de Internet y uso masivo de la computadora, se hace necesario la utilización de herramientas automatizadas que permiten la protección de documentos e información almacenada en las mismas (Granados, 2006). Algunas de estas utilidades son: los cortafuegos, los Sistemas Detectores de Intrusos y el uso de sistemas criptográficos; las mismas que permiten proteger tanto la información como a los Sistemas Informáticos encargados de administrarla.

✓ 3DES

Este algoritmo descendiente del algoritmo DES, diseñado por IBM y publicado en 1975, inicialmente estandarizado para instituciones

financieras, es actualmente uno de los algoritmos más utilizados por las tarjetas de crédito y otros medios de pago electrónico, no obstante, está desapareciendo lentamente debido a su proceso de cifrado que tiende a ser relativamente lento, y está siendo sustituido por el algoritmo AES, del cual a la fecha no se ha descubierto vulnerabilidades.

Este algoritmo se basa en doblar la longitud efectiva de la clave a 112 bits, pero debido a la necesidad de triplicar el número de operaciones necesarias la longitud total de la clave será de 168 bits, sin modificar el algoritmo DES (iso, 2018).

La Figura 1 presenta gráficamente cómo funciona el algoritmo 3DES con respecto a la gestión de su llave pública, y el proceso de cifrado y descifrado.

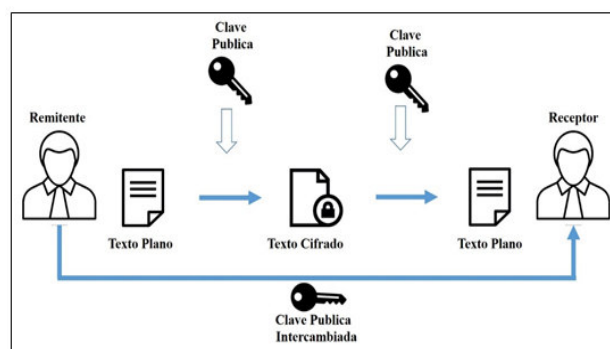


Figura 1. Funcionamiento del cifrado simétrico.
Fuente: (Arenas, 2016)

Por otro lado (Pousa, 2011), describe que 3DES utiliza un método llamado 3DES-Encrypt-Decrypt-Encrypt (3DES-EDE) para cifrar texto plano. Primero, el mensaje es cifrado utilizando

la primera clave de 56 bits, llamada K1, luego, los datos se descifran utilizando la segunda clave de 56 bits, llamada K2 y finalmente, los datos son nuevamente cifrados con la tercera clave de 56 bits, llamada K3.

En el siguiente grafico se muestra la Figura 2 y esta vez se presenta el funcionamiento del algoritmo 3DES con respecto al proceso de triple cifrado, tanto para cifrar el documento como para descifrarlo.

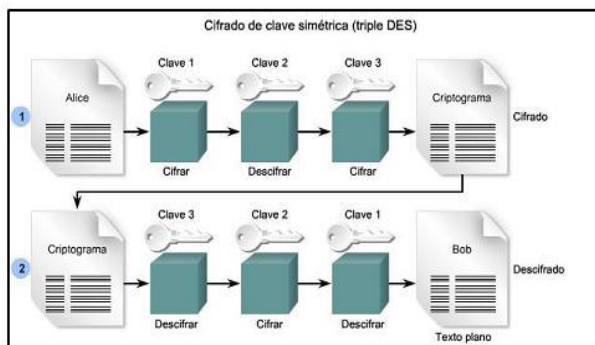


Figura 2. Algoritmo de cifrado Triple Des
Fuente: (Ariansen & Rojas, 2017)

✓ Rivest, Shamir y Adleman (RSA)

El algoritmo RSA es conocido por las iniciales de sus 3 descubridores (Rivest, Shamir y Adleman) y se estipula que este algoritmo se ha resistido a todos los intentos por romperlos por más de un cuarto de siglo, se le considera muy robusto (Lucena, 2014). Su mayor desventaja es que requiere de claves de al menos 1024 bits para garantizar mayor seguridad, en comparación con 128 bits de los algoritmos de clave simétrica, lo que lo vuelve relativamente lento.

El algoritmo RSA consta de tres pasos básicos: Generación de claves, cifrado y descifrado. La Figura 3 presenta gráficamente cómo funciona el algoritmo RSA con respecto a la gestión de su clave pública y su clave privada, y el proceso de cifrado y descifrado.

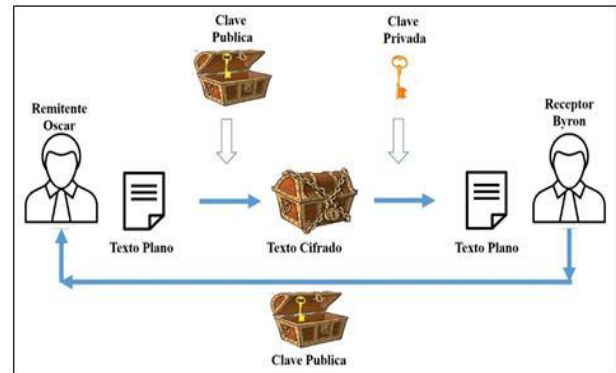


Figura 3. Funcionamiento del algoritmo asimétrico.
Fuente: (Lucena, 2014)

3 METODOLOGÍA

El presente trabajo se basa en una metodología con las siguientes características:

- ✓ **Investigación descriptiva:** El análisis que se dará, está enfocado a evaluar variables en entornos independientes para resaltar las características favorables y desfavorables de cada una, en cada uno de sus procesos.
- ✓ **Diseño experimental:** Pretende culminar con datos reales, demostrando de manera explicativa la relación causa-efecto.
- ✓ **Enfoque cuantitativo:** Debido a que se van a medir variables que determinarán al final de la investigación y rasgos importantes de cada uno de los algoritmos en sus

respectivos escenarios, sacando a la luz sus debilidades y fortalezas en lo que respecta a variables como asignación de seguridad, velocidad de procesamiento, costo de carga, entre otros factores que serán medidos en equipos con recursos muy limitados.

3.1 Población y muestra

Población

La población la constituye una empresa agrícola, con 83 plantas procesadoras y equipos Raspberry PI, los cuales están en producción de proceso de embalaje de fruta. En cada planta de proceso están 3 estaciones de trabajo con sus respectivos puntos de acceso a red inalámbricos, desde donde se envían los datos hacia el repositorio central ubicado en la ciudad de Guayaquil.

Muestra

La muestra fue seleccionada a través de un muestreo estratificado con afijación proporcional, utilizando las zonas como variable de estratificación. Los diferentes estratos n_h , se obtuvieron mediante la fórmula:

$$n_h = n \left(\frac{N_h}{N} \right) = nW_h$$

Donde:

N: 249 Tamaño de la población global objetivo

N_h : Tamaño de población proporcional

n: 25 Tamaño de la muestra global que se desea obtener

k: 0,1 Coeficiente de proporción

L: 6 Número de estratos

A partir de la cual se obtiene la distribución que se muestra en la Tabla 1:

Tabla 1. Distribución de la muestra

Estr.	Identificación	Host/ Estrato	Proporción	Muestra
1	Zona Norte 1	39	15,70%	4
2	Zona Norte 2	48	19,30%	5
3	Zona Centro 1	66	26,50%	6
4	Zona Centro 2	57	22,90%	6
5	Zona Sur 1	27	10,80%	3
6	Zona Sur 2	12	4,80%	1
Totales		249	99,80%	25

Fuente: Elaborado por el autor

3.2 Presentación del proyecto

Para la realización de la presente investigación se utilizará una plataforma tecnológica con dispositivos con características limitadas, microcomputadores de placa única que se encontraran formando parte de redes inalámbricas que se conectan a un repositorio central, donde se verificará la información enviada.

Con el analizador de protocolos se verificará los datos mientras están siendo enviados por la capa de transporte, comprobando el estado en que se encuentra, tanto en formato cifrado

como en formato de texto plano, y su contenido.

Se analizaron las pruebas de toma de datos en cada una de las respectivas empacadoras, de cada hacienda, en cada zona; efectuando 3 envíos desde el dispositivo Raspberry PI3 hasta el repositorio central, para luego de promediar, registrar dicho valor.

Se midió el tiempo que tarda el envío del archivo desde el dispositivo hasta llegar a un repositorio en la nube, tanto como texto plano, como cifrado con 3DES y RSA. En el transporte se verificó con Wireshark los datos del archivo, encabezado y valores de usuario y contraseña.

Adicionalmente a lo antes mencionado, se analizó la calidad de cifrado de los algoritmos sometidos a prueba y, por último, el porcentaje de crecimiento del archivo luego de haber sido cifrado con relación al archivo original.

Los resultados son presentados individualmente, por zona y globalmente, tanto en valores numéricos como en gráficos estadísticos que faciliten su comprensión y análisis.

Con el fin de alcanzar una geolocalización de las zonas y como están distribuidas a nivel nacional, se presenta a continuación sus ubicaciones a lo largo de las 5 provincias del

país, además de la distribución según el proveedor del servicio de enlace de última milla.

Aunque el proveedor del servicio de internet es uno solo, “Claro”, existen 2 proveedores diferentes que están brindando el servicio de enlaces de última milla (Nivel físico, antenas, radios, etc.), en la Figura 4 se puede ver que las zonas norte 1 y norte 2 están cubiertas por el proveedor del servicio de enlaces “Skyweb”, mientras que las demás zonas están con “Transdatel”.

Es importante, además, indicar que las zonas Norte 1 y Norte 2 mantienen un ancho de banda de 2 megas, mientras que las demás zonas están saliendo con un ancho de banda de 6 megas, y a pesar de que anteriormente no presentaban problemas de enlaces en las zonas Norte 1 y 2, desde que se está trabajando con el SBE sí se han estado presentando ciertos inconvenientes con varios usuarios con respecto a este tema.



Figura 4. Mapa de Planimetría Zonal.
Fuente: Elaborado por el autor

El archivo enviado desde los dispositivos Raspberry PI3 hasta el repositorio central, se encuentran en dos formatos diferentes:

- a) **Texto Plano.** En este formato será legible la información contenida, siendo posible la lectura de la información del archivo.
- b) **Texto cifrado.** En este formato la información contenida estará cifrada tanto con RSA como con 3DES, lo que imposibilitará la comprensión de los datos enviados.

En el archivo original, sin cifrar, se encuentran 2500 registros de cajas pesadas con todos sus componentes que lo integran, que es un promedio de las cajas que se procesan en todas las empacadoras diariamente. Además, tiene un tamaño de archivo de 572 Kb, y fue enviado desde cada uno de los hosts que se encuentran en las empacadoras, desde donde se envían hasta el repositorio central.

El archivo cifrado con 3DES, es el mismo archivo en texto plano que luego de ser procesado con el algoritmo 3DES se convierte en un archivo encriptado, que es ilegible durante su paso por la capa de transporte, y su tamaño varió dependiendo de los resultados del proceso de cifrado.

De igual manera, el archivo cifrado con RSA, es el archivo original que se cifra con el algoritmo RC4, que es una versión del RSA, y su tamaño también varió dependiendo de los resultados del proceso de cifrado. Estos archivos estarán siendo monitoreados durante su paso por la capa de transporte por el analizador de protocolos Wireshark, con el cual se verificó su contenido, además de otros parámetros.

Según la política de uso de los controles criptográficos definidos por la ISO 27001:2013, se implanta la protección de las llaves o claves de cifrado.

Una opción para la gestión de claves es KeePass, por estar bajo código libre y con licencia GNU GLPv2 está disponible para plataformas Linux, puede instalar la edición portátil de KeePass en una unidad de disco USB y guardarla en su bolsillo. No escribe ningún dato fuera de esa unidad, por lo que puede usarlo en cualquier computadora.

KeePass utiliza un inusual sistema de clave maestra compuesta que puede usar cualquiera o todos los tres métodos de autenticación distintos: contraseña maestra, archivo de clave y cuenta de usuario de Windows.

Las contraseñas deben ser largas y complejas. No necesariamente deben ser memorizadas, la


mayoría de los administradores de contraseñas incluyen un generador de contraseñas, pero muchos de ellos utilizan valores predeterminados deficientes. Norton, utiliza de forma predeterminada contraseñas alfanuméricas de ocho caracteres; Dashlane ofrece contraseñas de 12 caracteres de forma predeterminada, y Enpass Password Manager 5 tiene un máximo de 18 caracteres. KeePass, ofrece una contraseña predeterminada de 20 caracteres, lo que lo convierte en una buena opción.

4 RESULTADOS Y DISCUSIÓN

A continuación, se presenta el análisis comparativo entre las tecnologías de cifrado objeto de estudio.

4.1 Tamaño del archivo

Generalmente después de cifrar cualquier documento, es normal que se genere un ligero crecimiento de tamaño en el archivo original, y ese aumento en el tamaño del documento es importante que sea considerado por cuanto mientras más grande sea el archivo, más tiempo tardará en ser transferido desde el host hasta el repositorio. En la Figura 5 se exponen los resultados en cuanto al tamaño de archivo original y después de ser cifrado.



Nombre	tamaño	Fecha
2018-06-27-21-39-22-377.jpg	681.4 KB	2018-06-28 21:07:00
archivo.txt	571.0 KB	2018-11-27 15:58:00
archivo3DES.txt	2.2 MB	2018-11-27 20:43:00
archivoRC4.txt	1.5 MB	2018-11-27 20:42:00

Figura 5. Resultado de prueba de tamaño de archivo
Fuente: Elaborado por el autor

Se puede notar los tamaños de los archivos en el repositorio, tanto sin cifrar como después de haber sufrido el proceso de cifrado, lo que demuestra el incremento en el tamaño del archivo que es mayor por parte del cifrado 3DES sobre RSA.

Además de que el cifrado con RSA haya conseguido ser de menor tamaño, es importante indicar que por ser un cifrado asimétrico, el nivel de seguridad será también mayor al de un mecanismo de cifrado simétrico como lo es 3DES, sin dejar de nombrar que menor tamaño de archivo supone también menor carga de proceso para el dispositivo.

El archivo original que tenía un tamaño de 571 Kb, después del proceso de cifrado con el algoritmo RSA ha aumentado a 1,523 Kb, es decir un crecimiento del 167%; mientras que el mismo archivo en texto plano después del proceso de cifrado con el algoritmo 3DES ha alcanzado los 2,285 Kb, es decir, un crecimiento del 300%.

4.2 Tiempo de Carga de Archivo

Los 25 host utilizados en el estudio, están localizados en 6 zonas, de donde se toman las pruebas, y están ubicadas a lo largo de 4 provincias de la costa y 1 provincia de la sierra del país, además, se cuenta con 2 proveedores diferentes, el primero para las 2 zonas norte y el segundo para las demás zonas.

Zona Norte 1

Según podemos observar en el Gráfico 1, los resultados obtenidos en la zona norte 1, se presentan datos muy regulares, y considerando que el proveedor está ofreciendo 2 megas de velocidad, se puede visualizar que RC4 está siendo hasta ahora más rápido en presentar el acuse de recibido.

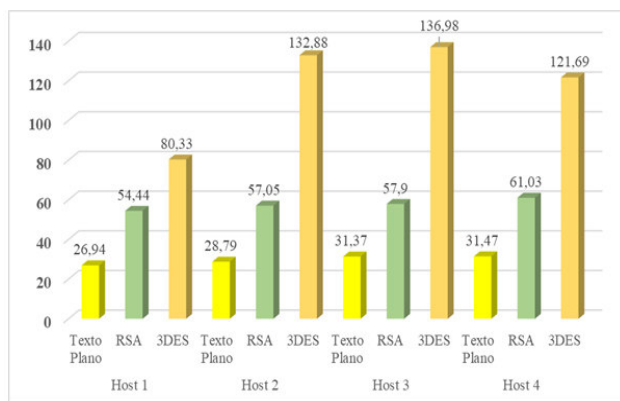


Gráfico 1. Resultados de Zona Norte 1
Fuente: Elaborado por el autor

Zona Norte 2

Los resultados de la zona Norte 2 está formada por 5 dispositivos, donde los resultados de las pruebas de tiempo de carga del archivo se

muestran tanto en texto plano, cifrados con RSA y cifrado con 3DES, y que son mostrados en la Gráfico 2.

Claramente se puede notar que el archivo cifrado con el algoritmo 3DES supera por mucho en el tiempo de envío hasta el repositorio al archivo cifrado con el algoritmo RSA, y se demuestra en cada caso, en cada uno de los hosts.

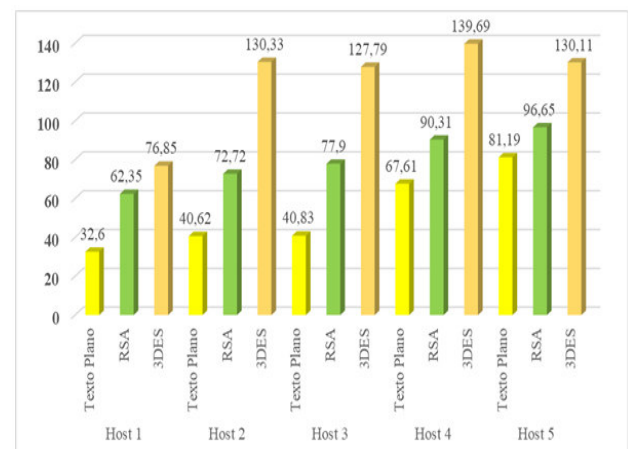


Gráfico 2. Resultados de Zona Norte 2
Fuente: Elaborado por el autor

Zona Centro 1

En el Gráfico 3 se presentan los resultados de las pruebas tomadas en la zona centro 1, con 6 hosts. En este caso debemos resaltar que se está trabajando con un proveedor de internet diferente al de las 2 zonas anteriores.

Los resultados de las pruebas registradas en la zona centro 1 muestran una gran diferencia en tiempos de respuesta en comparación con las zonas anteriores, donde se tiene un proveedor

de internet diferente, sin embargo, las diferencias entre los tiempos de envío entre los algoritmos de cifrado, se mantienen. En este caso, el RC4 sigue siendo más rápido en cuanto al envío del archivo cifrado.

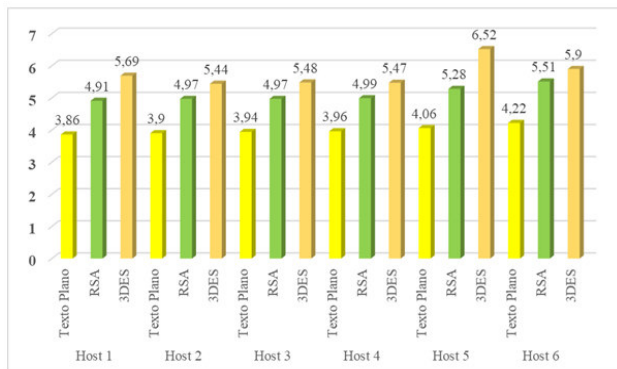


Gráfico 3. Resultados Zona Centro 1
Fuente: Elaborado por el autor

Zona Centro 2

A continuación, se muestra la Gráfico 4 con el resumen de los resultados de las pruebas realizadas en la zona centro 2, donde se puede comprobar una concordancia con los resultados obtenidos en la zona centro 1, a cargo del mismo proveedor de internet. Los porcentajes en tiempos de envío siguen manteniéndose, dejando ver que RSA es más rápido en cuanto al proceso de cifrado y envío del documento hasta el repositorio central.

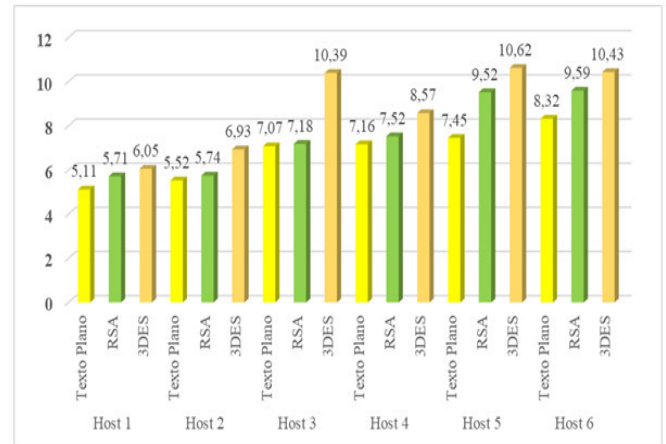


Gráfico 4. Resultados de Zona Norte 2
Fuente: Elaborado por el autor

Zona Sur 1

En el Gráfico 5 muestran los resultados de las pruebas realizadas en la zona sur 1, coincidiendo con los resultados de las zonas anteriores, manteniendo tiempos de envío mucho menores que las zonas norte 1 y 2, pero sosteniendo la brecha entre los algoritmos RSA y 3DES.

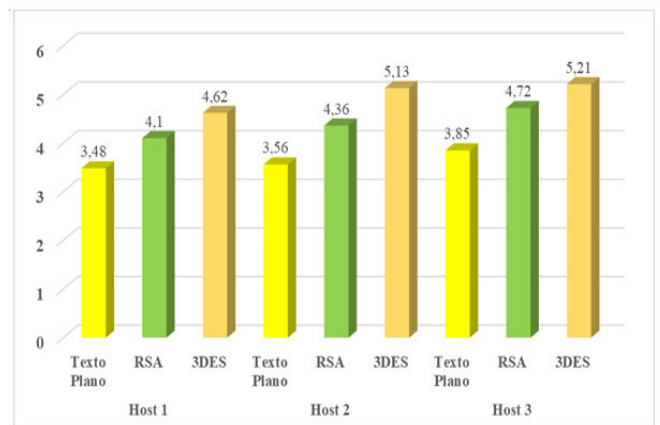


Gráfico 5. Resultados de Zona Sur 1
Fuente: Elaborado por el autor

Zona Sur 2

En el Gráfico 6 se muestra el resultado tomado del único host de prueba de la zona sur 2,

presentando datos parecidos a los obtenidos anteriormente. Los resultados presentados dejan ver una vez más en claro que el algoritmo RSA demuestra ser el mecanismo de cifrado con mejor tiempo de respuesta en el proceso de envío de la información.

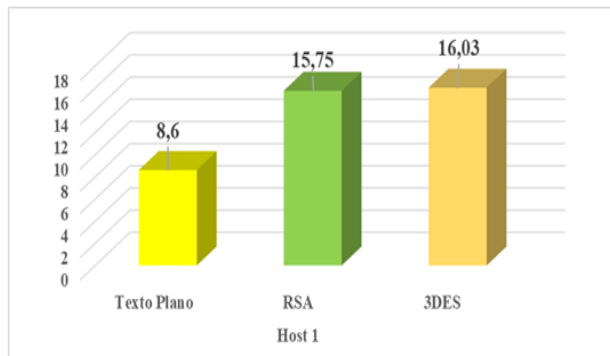


Gráfico 6. Resultados de Zona Sur 2
Fuente: Elaborado por el autor

Resumen de tiempos de carga al repositorio

Durante el proceso de levantamiento de la información, resultado de las pruebas realizadas en los diferentes dispositivos de las 6 zonas, se ha logrado notar que en las zonas norte 1 y 2 que están con el proveedor de internet número 1, los tiempos de entrega de la información son mucho más altos que los tiempos de respuesta de las zonas centro 1 y 2 y sur 1 y 2, que están con el proveedor de internet número 2.

El promedio de todos los resultados obtenidos durante el proceso de pruebas, representado por la Gráfico 7, demuestra que, el cifrado con el algoritmo RSA se presenta con 29,4 segundos, mientras que 3DES se presenta con

47,8, lo que, en comparación con el promedio del tiempo de envío del archivo en texto plano que es 18,6 segundos, deja como resultado lo siguiente:

- ✓ El algoritmo RSA incremento el tiempo de respuesta durante el envío del archivo cifrado desde los dispositivos Raspberry hasta el repositorio central en un 58%.
- ✓ El algoritmo 3DES incremento el tiempo de respuesta durante el envío del archivo cifrado desde los dispositivos Raspberry hasta el repositorio central en un 157%.

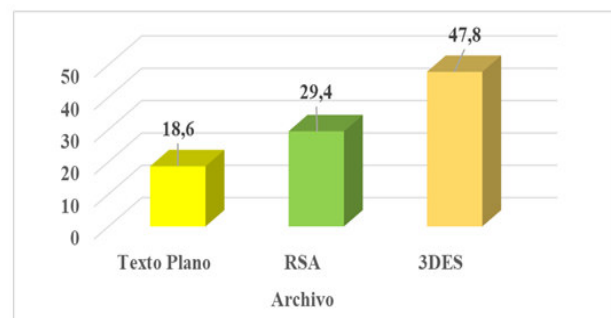


Gráfico 7. Resultados promediados de las 6 zonas.
Fuente: Elaborado por el autor

5 CONCLUSIÓN

Luego del análisis de la información obtenida durante la investigación, se puede concluir lo siguiente:

En internet existen muchos sitios, ya sea en bibliotecas en línea, foros de investigación, y en muchos otros portales de interés científico, donde se encuentra información sobre investigaciones realizadas, y se compara variados algoritmos de encriptación, en los que

se mide no solo la velocidad de proceso, sino también vulnerabilidad del cifrado, e incluso la capacidad de resistir los ataques de diversos programas para romper la seguridad del cifrado, y siempre se lo hace en equipos computacionales robustos con memorias de hasta 32 Gb de memoria RAM y con procesadores de última generación, sin embargo, estas mismas investigaciones no se las ha realizado en dispositivos con recursos limitados como lo son los dispositivos de placa única Raspberry Pi o Arduino.

En las pruebas realizadas a los 25 hosts, evidencia que el algoritmo asimétrico de cifrado RC4, variante ultima a la fecha de la realización de esta investigación, supera en un 100% con 29,4 segundos al cifrado con el algoritmo 3DES, que tardó 47,8 segundos, con respecto al tiempo de proceso de cifrado del archivo en texto plano que contiene la información del proceso diario de las haciendas donde se realizaron las pruebas, comparados ambos con el envío del archivo en texto plano que tardó 18,6 segundos en entregarse en el repositorio central de la empresa.

Es importante aclarar que, en el tiempo de carga del archivo se tiene que considerar el tiempo que tarda el algoritmo en efectuar el proceso de cifrado, lo que demuestra que el

algoritmo RSA es más rápido en cuanto a este proceso que el algoritmo 3DES.

Además de haber obtenido un mejor tiempo durante el envío, RC4 también logró un tamaño del archivo cifrado menor que 3DES, es decir, RC4 se incrementó en un 167% con 1,5 Mb, mientras que 3DES se incrementó en un 300% su tamaño con 2,2 Mb, ambos en relación al tamaño del archivo en texto plano que pesaba 0,571 Mb.

Otro punto importante que se debe anotar es que, el algoritmo 3DES utiliza claves de 112 bits de longitud, mientras que RSA utiliza claves de al menos 1024 bits, lo que deja claro que es más robusto en cuanto a seguridad.

Sin embargo, pese a la información obtenida en esta investigación, se debe aclarar que, en cualquier caso, será la gerencia del área de TI quien finalmente decida sobre tal o cual sistema de cifrado aplicar para el área de trabajo.

6 RECOMENDACIONES

Realizar las pruebas en otras plataformas como dispositivos HummingBoard, que presenta características de hardware similares a Raspberry Pi, igualmente BeagleBone Black y Odroid U3 que llega a alcanzar las 2 GB de memoria RAM, para confirmar los resultados, siendo estos también microordenadores de

placa única, los resultados podrían contrastarse con los obtenidos en la presente investigación.

Con el fin de alcanzar un mayor grado de seguridad, incorporar otros algoritmos de cifrado como AES y combinarlos con los utilizados en la presente investigación y comparar los resultados.

Utilizar otros tipos de archivos de mayor tamaño durante el proceso de pruebas, como imágenes, pdf, audios y videos, que tengan tamaños superiores a los utilizados en la presente investigación.

7 REFERENCIAS

- Arenas, X. (16 de Octubre de 2016). *Sistemas Distribuidos y Seguridad Web*. Obtenido de <http://sistemasdistribuidosyseguridadweb.blogspot.com/2016/10/cifrado-simetrico-firmas-sellos-y.html>
- Ariansen, R., & Rojas, J. (2017). *Implementacion de Protocolo de Cifrado TLS para mejorar la Seguridad de la capa de Transporte*. Chiclayo: Universidad Señor de Sipan.
- González, K., & Urrego, G. (2014). Estudio sobre Computadores de Placa Reducida Raspberry Pi Modelo B y Cubieboard2. *ENGI*, 6-10.
- Granados, G. (2006). Introducción a la criptografía. *Revista Digital Universitaria*, 1-17.
- iso. (20 de Septiembre de 2018). www.iso27000.es. Obtenido de <http://www.iso27000.es/iso27000.html>
- Lucena, M. (2014). *Criptografía y Seguridad en Computadores*. Sevilla: Openlibra.
- Pousa, A. (2011). *Algoritmo de cifrado simétrico AES. Aceleración del tiempo de cómputo sobre arquitectura multicore*. La Plata: Universidad Nacional de La Plata. Obtenido de https://virtual.itca.edu.sv/Mediadores/cms/u63_esquema_general_de_un_sistema_de_cifrado_simtrico.html