



**REPÚBLICA DEL ECUADOR**

**VICERRECTORADO DE INVESTIGACIÓN Y  
POSGRADO**

**PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL  
TÍTULO DE:**

**MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN**

**TÍTULO DEL PROYECTO:**

**IMPLEMENTACIÓN DE UN MECANISMO DE  
ENCRIPCIÓN ASIMÉTRICO PARA MEJORAR LA  
SEGURIDAD DENTRO DEL DEPARTAMENTO DE  
SERVIDORES DEL ISP IN.PLANET S.A DE LA CIUDAD DE  
MILAGRO**

**TUTOR**

**PhD. JORGE RODAS SILVA**

**AUTOR**

**GERARDO DAVID ANDRADE TOSCANO**

**MILAGRO, 2023**



## VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO

Milagro, 30 de octubre, 2023

### CERTIFICACIÓN DE ACEPTACIÓN DEL TUTOR

En calidad de Tutor del Proyecto de Investigación, nombrado por el Comité Académico del Programa de Maestría en Tecnologías de la Información de la Universidad Estatal de Milagro.

### CERTIFICO

Que he analizado el Proyecto de Investigación con el tema **IMPLEMENTACIÓN DE UN MECANISMO DE ENCRIPCIÓN ASIMÉTRICO PARA MEJORAR LA SEGURIDAD EN EL DEPARTAMENTO DE SERVIDORES DEL ISP IN.PLANET S.A DE LA CIUDAD DE MILAGRO**, elaborado por **ANDRADE TOSCANO GERARDO DAVID**, el mismo que reúne las condiciones y requisitos previos para ser defendido ante el tribunal examinador, para optar por el título de **MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN**.



Firmado electrónicamente por:  
**JORGE LUIS  
RODAS  
SILVA**

**RODAS SILVA JORGE LUIS, PhD.**

**C.I: 0921633988**



## DECLARACIÓN DE AUTORÍA DE LA INVESTIGACIÓN

El autor de esta investigación declara ante el Comité Académico del Programa de Maestría en Tecnologías de la Información de la Universidad Estatal de Milagro, que el trabajo presentado es de mi propia autoría, no contiene material escrito por otra persona, salvo el que está referenciado debidamente en el texto; parte del presente documento o en su totalidad no ha sido aceptado para el otorgamiento de cualquier otro título de una institución nacional o extranjera.



Firmado electrónicamente por:  
ANDRADE  
TOSCANO  
GERARDO DAVID

**ANDRADE TOSCANO GERARDO DAVID**  
**C.I: 094219290-7**

**VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO**  
**DIRECCIÓN DE POSGRADO**  
**CERTIFICACIÓN DE LA DEFENSA**

El TRIBUNAL CALIFICADOR previo a la obtención del título de **MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN**, presentado por **ING. ANDRADE TOSCANO GERARDO DAVID**, otorga al presente proyecto de investigación denominado "IMPLEMENTACIÓN DE UN MECANISMO DE ENCRIPCIÓN ASIMÉTRICO PARA MEJORAR LA SEGURIDAD EN EL DEPARTAMENTO DE SERVIDORES DEL ISP IN.PLANET S.A DE LA CIUDAD DE MILAGRO", las siguientes calificaciones:

TRABAJO DE TITULACION	57.33
DEFENSA ORAL	40.00
<b>PROMEDIO</b>	<b>97.33</b>
<b>EQUIVALENTE</b>	<b>Excelente</b>



firmado electrónicamente por:  
**DENIS DARIO MENDOZA  
CABRERA**

---

**Mgti. MENDOZA CABRERA DENIS DARIO**  
**PRESIDENTE/A DEL TRIBUNAL**



firmado electrónicamente por:  
**LUIS CRISTOBAL  
CORDOVA MARTINEZ**

---

**M.A.E. CORDOVA MARTINEZ LUIS CRISTOBAL**  
**VOCAL**



firmado electrónicamente por:  
**MARIUXI GEOVANNA  
VINUEZA MORALES**

---

**Ph.D. VINUEZA MORALES MARIUXI GEOVANNA**  
**SECRETARIO/A DEL TRIBUNAL**

## **AGRADECIMIENTO**

Agradezco a DIOS, mi padre celestial que es quien escucha mis oraciones y me protege durante todo mi camino. Es él quien me da la sabiduría y la fortaleza necesaria para concluir con éxito mi proyecto de tesis.

Agradezco de todo corazón a mis padres que son pilar fundamental en mi vida y gracias a ellos en conjunto con mis hermanos, me han dado ese empuje y apoyo incondicional desde el inicio de esta maestría y han logrado que no me derrumbara ante los obstáculos y dificultades que se me presenten.

Un agradecimiento muy especial a mi tutor PhD. Jorge Rodas S., quien amable y pacientemente con su conocimiento y experiencia me ha guiado, me ha corregido y ha tenido toda la predisposición de ayudarme en la elaboración de este proyecto.

Agradezco a mi gran amiga Diana Herán quien, con sus consejos, su apoyo y sus palabras de aliento, me han dado valor para seguir en pie de lucha desde el inicio de mi tesis.

Agradezco también a compañeros como Leonardo y Dario Piña Campoverde, que me han brindado el soporte en ciertas dificultades presentadas en la tesis, por permitirme el acceso y por su experiencia adquirida en el departamento de servidores de In.planet S.A.

# DEDICATORIA

Con toda la humildad que de mi corazón puede emanar, en primer lugar, dedico mi trabajo a DIOS, porque es él quien me ha dado esas fuerzas para continuar y no dejar que me derrumbe por nada.

A mis queridos padres Freddy y Eulalia por ser mi motor y mi mayor inspiración, quienes me han dado esa confianza y han creído siempre en mí. Por ese apoyo y empuje que siempre necesita un hijo de sus padres.

A mis 2 hermanos por su cariño y confianza, por ser las personas que siempre han estado a mi lado dándome consejos valiosos e importantes. Por ser ese ejemplo de amor y trabajo duro, son sin duda alguna lo mejor de lo mejor.

Por último, pero no menos importante dedico mi proyecto de tesis a mis abuelitos Luis y Mercedes por quererme y apoyarme en todo momento. Por ser mis consejeros y ejemplos a seguir, esto también es para ustedes.

## RESUMEN

El presente proyecto se centra en dar solución a la problemática que enfrenta el departamento de servidores de In.Planet S. A., en su sede en el edificio HEY!, ubicado en la ciudad de Milagro entre las calles Malecón 312 y Federico Proaño, sobre la seguridad de la información. La solución más viable fue implementar el mecanismo de encriptación asimétrico RSA<sup>1</sup>, mismo que mediante el uso de las llaves generan una mayor seguridad. Además, se incorporó una medida extra de seguridad en la fase de optimización, la cual constó de la instalación de un servidor en donde se incorporó las llaves RSA. Además, en el server a administrar se añadió reglas de firewall<sup>2</sup> que solo permiten la conexión desde el servidor master.

### **Palabras clave:**

SSH, protocolo ssh, mecanismos de encriptación asimétrica, servidores, soporte, administración, llaves públicas, llaves privadas.

---

<sup>1</sup> Sistema criptográfico asimétrico, su nombre se debe a las siglas de sus tres fundadores (Rivest, Shamir y Adleman).

<sup>2</sup> Comprende de un sistema de seguridad de red de las computadoras que inhabilita el tráfico de Internet entrante, saliente o dentro de una red privada.

## **ABSTRACT**

This research project focuses on providing a solution to the problem faced by the server department of In.Planet S. A., at its headquarters in the HEY! building, regarding information security. The most viable solution was to implement the RSA asymmetric encryption mechanism, which through the use of keys generates greater security. In addition, as an extra security measure, optimizations were carried out, for this a server was installed in which the RSA keys were installed, also on the server to be managed, firewall rules were added that only allow the connection from the master server.

**Keywords:**

SSH, protocol ssh, asymmetric encryption mechanisms, servers, support, administration, public keys, private keys.



# ÍNDICE

<b>INTRODUCCIÓN .....</b>	<b>1</b>
<b>CAPÍTULO 1.....</b>	<b>2</b>
1.1. Planteamiento del problema .....	2
1.2. Objetivos .....	3
1.3. Alcance .....	5
1.4. Estado del arte .....	5
<b>CAPÍTULO 2.....</b>	<b>16</b>
2.1. Metodología.....	16
<b>CAPÍTULO 3.....</b>	<b>19</b>
3.1. Propuesta de solución.....	19
<b>3.2. Fase 1: Preparar. ....</b>	<b>19</b>
3.2.1. Departamento de servidores: .....	19
3.2.2. Dispositivos de enlace a los servidores. ....	22
3.2.3. Encargado del departamento de servidores. ....	23
3.2.4. Análisis económico.....	24
<b>3.3. Fase 2: Planificar.....</b>	<b>25</b>
3.3.1. Necesidades para cada equipo: .....	25
3.3.2. Especificidades de requerimientos solicitados:.....	27
<b>3.4. Fase 3: Seleccionar.....</b>	<b>28</b>
3.4.1. Características y comparación entre RSA, DSA y ElGamal.....	29
3.4.2. Evaluación de los mecanismos de encriptación asimétricos para la aplicación para las medidas de seguridad del departamento de servidores.....	30
<b>3.5. Fase 4: Diseñar.....</b>	<b>32</b>
3.5.1. Arquitectura del funcionamiento del mecanismo de encriptación.....	32
<b>3.6. Fase 5: Optimizar. ....</b>	<b>39</b>
3.6.1. Capa extra de seguridad. ....	39
<b>CONCLUSIONES Y TRABAJO FUTURO.....</b>	<b>50</b>
<b>RECOMENDACIONES .....</b>	<b>51</b>
<b>BIBLIOGRAFÍA GENERAL: .....</b>	<b>52</b>

<b>ANEXOS</b> .....	<b>54</b>
Anexo 1.....	54
Anexo 2.....	54

## ÍNDICE DE ILUSTRACIÓN

Ilustración 1: Sistema Criptográfico RSA.....	12
Ilustración 2: Metodología PPSDO.....	16
Ilustración 3: Servidor Supermicro ESXI 01.....	20
Ilustración 4: Servidor Supermicro ESXI 02.....	20
Ilustración 5: Servidor Supermicro ESXI 03.....	20
Ilustración 6: Servidor Supermicro ESXI 04.....	21
Ilustración 7: Servidor Supermicro ESXI 05.....	21
Ilustración 8: Servidor Supermicro ESXI 06.....	21
Ilustración 9: Servidor DELL ESXI 7.....	21
Ilustración 10: Servidor DELL ESXI 8.....	21
Ilustración 11: Servidor DELL ESXI 9.....	22
Ilustración 12: Servidor DELL ESXI 10.....	22
Ilustración 13: Servidor HP ESXI 11.....	22
Ilustración 14: Servidor HP ESXI 12.....	22
Ilustración 15: Dispositivos de enlace a los servidores.....	23
Ilustración 16: Diseño de la arquitectura de la propuesta de solución.....	32
Ilustración 17: Comando que genera el par de llaves SSH, una privada y una pública.....	33
Ilustración 18: Pedirá que se les dé un nombre a los archivos en caso de dejarlo por defecto se dará enter y se guardaran como id_rsa.....	33
Ilustración 20: La llave fue generada con éxito.....	33
Ilustración 21: Nos ubicaremos en el directorio donde se alojan las llaves SSH creadas. .	34
Ilustración 22: llave privada id_rsa y llave pública id_rsa.pub.....	34
Ilustración 23: Si se abre el archivo podremos ver el contenido de la llave.....	35
Ilustración 24: Ingresaremos al servidor para configurar las llaves y el servicio OpenSSH.	35
Ilustración 25: Escalaremos de privilegios.....	36
Ilustración 26: Modificaremos el archivo sshd_config.....	36
Ilustración 27: Buscaremos la línea PasswordAuthentication que por defecto está comentada.....	37
Ilustración 28: La descomentaremos y cambiaremos el yes por no.....	37
Ilustración 29: Reiniciaremos el servicio de SSH.....	38
Ilustración 30: Ingresaremos al directorio de llaves del usuario y modificaremos el archivo authorized_keys.....	38
Ilustración 31: Pegaremos el contenido del arhico id_rsa.pub y guardaremos.....	38
Ilustración 32: Iniciaremos sesión nuevamente en el server y esta vez pedirá la clave de la llave SSH.....	39
Ilustración 34: Instalamos un nuevo servidor.....	40
Ilustración 35: Identificaremos la llave privada.....	41
Ilustración 36: Una vez instalado el nuevo servidor copiaremos la llave privada a dicho servido.....	41
Ilustración 37: La llave se copiará en la ruta indicada.....	42
Ilustración 38: Cambiaremos el nombre del archivo.....	42
Ilustración 39: Realización de un cat para ver el contenido de la llave privada.....	43
Ilustración 41: Generar otro par de llaves que permitirá la conexión al servidor máster. ...	43
Ilustración 42: Los archivos fueron creados.....	44
Ilustración 43: Contenido de la llave pública.....	44
Ilustración 44: Edición del archivo de llaves autorizadas en el nuevo servidor.....	45
Ilustración 45: Pegaremos el contenido de la llave pública.....	45
Ilustración 46: Edición del archivo de configuración de SSH.....	45
Ilustración 47: Modificaremos la línea tal como se muestra en la imagen.....	45

Ilustración 49: Cambio de los permisos de la llave. ....	46
Ilustración 50: Ingresaremos al servidor que anteriormente se había configurado la llave SSH id_rsa.....	46
Ilustración 51: Comprobaremos el estado del firewall de dicho servidor.....	47
Ilustración 52: Permisos de conexión al puerto 22 solo a la ip indicada que es la ip del servidor master. ....	47
Ilustración 53: Habilitaremos el firewall y comprobaremos la regla añadida. ....	47
Ilustración 55: Tener en cuenta que, con llave o sin llave no nos permitirá el acceso ya que solo se dio permiso a la ip del servidor master .....	48
Ilustración 56: Iniciamos sesión en el servidor master.....	48
Ilustración 57: Comprobación del acceso al servidor.....	49

## ÍNDICE DE TABLAS

Tabla 1: Características generales de servidores.....	20
Tabla 2: Funciones del Técnico DataCenter Software del departamento de servidores de In.Planet S.A. ....	24
Tabla 3: Costos del tiempo de implementación basado en las horas laborales del Técnico DataCenter Software.....	25
Tabla 4: Servidores Supermicro y sus respectivas Máquinas Virtuales a las cuales se aplicará el respectivo mecanismo de encriptación asimétrico.....	26
Tabla 5: Servidores DELL y sus respectivas Máquinas Virtuales a las cuales se aplicará el respectivo mecanismo de encriptación asimétrico.....	27
Tabla 6: Servidores HP y sus respectivas Máquinas Virtuales a las cuales se aplicará el respectivo mecanismo de encriptación asimétrico.....	27
<i>Tabla 7: Análisis de necesidades del departamento de servidores.....</i>	<i>28</i>
<i>Tabla 8: comparativa de características entre los mecanismos de encriptación asimétrica RSA, DSA y ElGamal.....</i>	<i>30</i>
<i>Tabla 9: Evaluación de los mecanismos de encriptación asimétricos RSA, DSA y ElGamal.....</i>	<i>31</i>

# INTRODUCCIÓN

El protocolo SSH (Secure Shell) es actualmente uno de los servicios más utilizados para la conexión y administración de servidores basados en Linux, el protocolo es seguro, sin embargo actualmente se han encontrado fallas de seguridad en el mismo, las cuales han sido parchadas (corregidas), el principal temor de los administradores de sistemas es que en algún momento aparezcan ataques zero day (ataques sin precedentes o de día cero), por ende se ha evaluado varias maneras de dar una capa mayor de seguridad al protocolo.

El presente proyecto aplicado previo a la obtención del título de master en tecnologías de información propone la implementación de una capa de seguridad basada en un sistema de llaves usando un sistema de cifrado asimétrico. Para lo cual se optó por la utilización de llaves ssh en conjunto con sistema de cifrado, se han evaluado tres alternativas de sistemas de cifrado, de los cuales se seleccionó el que mejor se adaptaba a los requerimientos del técnico de datacenter software, que es la persona encargada, de instalar, administrar y monitorizar, todos los servidores de la ISP (proveedor de servicios de internet) In.Planet S.A. de la ciudad de Milagro.

# CAPÍTULO 1

## 1.1. Planteamiento del problema

En el contexto actual, las redes de comunicación cumplen un rol fundamental en la interconectividad en la que se comparte una gran cantidad de información, misma que es transmitida y receptada desde diferentes medios, lo cual implica ciertos riesgos de vulnerabilidad al compartir dichos contenidos.

En relación a los riesgos de vulnerabilidad, podemos encontrar al factor humano, que es el eslabón más débil dentro de la seguridad informática, ya que el usuario tiende a usar contraseñas con referencia a fechas, mascotas, familiares, etc., que mediante el uso de ingeniería social es posible la obtención de las credenciales de acc

eso. De igual manera existen precedentes en las que el usuario guarda en block de notas o cuadernos las contraseñas usadas.

De la misma manera podemos encontrarnos con ataques man-in-the-middle donde el intruso se interpone entre el usuario y el dispositivo y realiza captura en todo el tráfico. También podemos encontrarnos con ataques añadidos, como dns spoofing que intercepta la comunicación y re-direcciona el tráfico de comunicación hacia un servidor malicioso y de esta manera capturar las credenciales de acceso.

En el caso de ataques de fuerza bruta, es el cual comprende un intento por descifrar la contraseña o el nombre del usuario mediante un método de prueba y error hasta identificar las credenciales que se han propuesto encontrar. Este tipo de ataque

informático es más sencillo de detectarlo y bloquearlos, ya que el servidor estará recibiendo esta información en el log o archivos de registros varias peticiones de inicio de sesión fallidas. Lo más común en este tipo de ataque se complementa con los ataques de diccionarios que, contiene palabras comunes, así como combinación de letras y números. A pesar de ser relativamente fácil de detectar este tipo de ataque informático, no exenta la posibilidad de ser vulnerados.

## **1.2. Objetivos**

### **1.2.1. Objetivo General**

Implementar medidas de seguridad para el departamento de servidores de IN. PLANET S.A., mediante el uso de un mecanismo de encriptación asimétrico para evitar vulnerabilidades y garantizar confidencialidad, integridad y autenticidad de los datos transmitidos en entornos de redes de comunicaciones.

### **1.2.2. Objetivos Específicos**

- Indagar sobre los diferentes mecanismos de encriptación para la seguridad en redes de comunicación existentes en el mercado.
- Evaluar la resistencia de los mecanismos de encriptación asimétrica frente a ataques criptoanalíticos y de fuerza bruta, y proponer medidas de protección adicionales, posibles vulnerabilidades y debilidades en dichos mecanismos.



- Seleccionar el mecanismo de encriptación más eficiente que proporcionen mejoras en la seguridad en las redes de comunicaciones.

### **1.3. Alcance**

Para resolver la problemática de vulnerabilidad en el departamento de servidores del Proveedor de Servicios de Internet In.Planet. S. A., el presente proyecto se tiene como alcance la implementación de medidas de seguridad basadas en mecanismos de encriptación asimétricos, los cuales brindarán una mayor capa de seguridad.

Los mecanismos de encriptación asimétricos que se utilizarán como medidas de seguridad permitirán a los usuarios encargados del departamento de servidores, llevar un mejor control ante posibles vulnerabilidades, como factor humano, ataques criptoanalíticos, man-in-the-middle, dns spoofing o ataques de fuerza bruta. Y de esta manera garantizar la confidencialidad, integridad y autenticidad de la información transmitida de la ISP. Estos mecanismos serán aplicados bajo la normativa ISO/IEC 27001 en consonancia con el protocolo SSH y el Software OpenSSH en el sistema operativo Linux.

### **1.4. Estado del arte**

El elemento circunstancial para el funcionamiento de una empresa recae en la información y la operación del negocio, lo cual nos lleva a la decisión de proteger dicha información y considerándola como el activo más relevante de la empresa. En el contexto tecnológico actual, el incremento de la participación de internet en los procesos comunicacionales ha provocado un sinnúmero de amenazas que representa riesgos en la vulnerabilidad de la información para las empresas. Dichas

vulnerabilidades ocasionan que la información se vea comprometida y se pierda la disponibilidad, integridad y la confidencialidad. Argüezo Ramirez, E. D. (2019) menciona que:

Siempre que platicamos de una empresa, institución, organismo o entidad entre otras organizaciones similares, es importante que la información que se encuentre integrada en ellas esté resguardada bajo unas buenas medidas de seguridad. Es ahí donde brota la seguridad de la información para mantener a salvo todos los datos importantes de la empresa, desde los que pertenecen a la propia organización como los vinculados con trabajadores y clientes. A veces nos equivocamos este tipo de seguridad con la seguridad informática, pero hay que tener en cuenta que esta última solo se centra en salvaguardar los datos dentro de un sistema informático, mientras que la información en general puede darse en otros muchos contextos entre los usuarios. (PP. 43-44)

La seguridad de la información según lo estipula la normativa ISO/IEC 27001 establecida en el 2013, hace referencia a tres dimensiones para salvaguardar la seguridad de la información. Estas tres dimensiones son la confidencialidad, integridad y disponibilidad de los que una empresa posee. Fernández Orozco. (2021) menciona que:

La información que posee cualquier tipo de organización constituye uno de los activos más importantes, por lo tanto, dicha organización debe contar con las herramientas y estrategias necesarias para mitigar o eliminar los

riesgos a los que podrían estar expuestos y asegurar así la continuidad del negocio. (P.22)

**Confidencialidad:** “la información no se pone a disposición ni se revela a personas no autorizadas. En necesario implementar controles de acceso para la identificación, autenticación y autorización” (Fernández Orozco, 2021, p. 23).

**Integridad:** “se debe salvaguardar la totalidad y exactitud de la información que se gestiona, existe casos en el que la información se ha visto alterada por errores humanos, entre ellos se puede ejemplificar el borrado o modificación de archivos (...)” (Fernández Orozco, 2021, p. 23).

**Disponibilidad:** “es el acceso y utilización de la información por parte de personas autorizadas en el momento que así lo requieran” (Fernández Orozco, 2021, p. 23).

#### **ISO:**

Argüeso Ramirez, E. D. (2019) “Las siglas ISO representan a la Organización Internacional para la Estandarización; organismo responsable de regular un conjunto de normas para la fabricación, comercio y comunicación en todas las industrias y comercios del mundo” (p. 72). Argüeso Ramirez, E. D. (2019) agrega que:

En la actualidad la ISO tiene su sede en Ginebra, Suiza y cuenta con delegaciones de diversos gobiernos y otros entes similares. Sin embargo, y a pesar de su alta influencia a nivel mundial, el acatamiento de estas normas es

de manera voluntaria, ya que la ISO no tiene poder para imponer sus regulaciones.

### **Normativa ISO 27001.**

La normativa ISO 27001 hace referencia a la gestión de la seguridad de la información. Fernández Orozco. (2021) dice que:

La ISO 27001 es una norma internacional emitida por la ISO y describe cómo gestionar la seguridad de la información en una organización. La primera revisión se publicó en 1998 y fue un estándar nacional británico certificable BS 7799-2. La versión más actual fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013.

Su última actualización corresponde al año 2022 con el con el nombre ISO 27001:2022.

### **Estructura de la Norma ISO/IEC 27001:2022**

De la misma forma que la mayor parte de las Normas de Sistemas de Gestión ISO, los requerimientos de la normativa ISO 27001 se debe cumplir. La normativa ISO/IEC 27001 cuenta con 10 clausula La ISO 27001:2022 sigue la estructura de alto nivel (NQA, 2022).

1. Alcance
2. Referencias normativas
3. Términos y definiciones

4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del rendimiento
10. Mejora

### **Protocolo SSH:**

SSH o Secure Shell, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet mediante un mecanismo de autenticación. Enrique Bonet. (2023) menciona que:

Secure SHell es un protocolo que permite crear conexiones seguras entre dos ordenadores. Usando SSH, la máquina del cliente inicia una conexión con la máquina del servidor mediante una sesión cifrada, imposibilitando que alguien pueda obtener una contraseña o cualquier otro tipo de información que se envíe por la red (P. 1)

Además, SSH está diseñado para sustituir los métodos comunes de acceso remoto a un decodificador de comandos de otro dispositivo, como el caso de Rlogin o Telnet, al igual que otros programas destinados a copiar ficheros entre dispositivos como por ejemplo RCP o FTP, ya que estas aplicaciones no cifran las contraseñas entre el cliente y el servidor (Enrique Bonet, 2023)

### **Software OpenSSH:**

“SSH (...) es una herramienta para la administración segura del sistema, transferencias de archivos y otras comunicaciones a través de Internet u otra red no confiable. Cifra identidades, contraseñas y datos transmitidos para que no puedan ser espiados y robados” (SSH, 2023, párr. 1) “OpenSSH es una implementación de código abierto del protocolo SSH. Está basado en la versión gratuita de Tatu Ylonen y desarrollado por el equipo de OpenBSD y la comunidad de usuarios” (SSH, 2023, párr. 1).

### **Criptografía:**

“(...). Es la base de la identidad, la privacidad y la seguridad en línea. Solo la aplicación cuidadosa y bien ejecutada de la criptografía permitirá mantener la información privada oculta de ojos y oídos indiscretos” (SSH, 2023, párr. 1).

La criptografía es la técnica que se encarga del cifrado y el codificado de los datos con la finalidad de hacerlos inteligibles a personas y terceros para los que no está destinado el mensaje. Esta técnica se utiliza en el arte, la tecnología y en la ciencia para conseguir que los mensajes sean confidenciales. (INESDI, 2021, párr. 1)

### **Encriptación asimétrica:**

La encriptación asimétrica está basada en el uso de dos claves; pública y privada. En relación a pública se podrá difundir sin problema a todo el personal que necesite mandar información cifrada, y por consiguiente la clave privada no debe de ser revelada, debe estar resguardada bajo la supervisión del personal de seguridad

de la información. Como lo menciona Cabrera Serrano, X. A. (2023). “Este método de cifrado bastante nuevo, y según la historia cuenta que se basaba en utilizar claves distintas para cifrar y para descifrar un mensaje permitiendo cifrar una clave pública que cualquier persona puede conocer” (p. 9).

Cabanillas Urbina, H. A., & Nizama Ramos, J. J. V. (2022). “El cifrado asimétrico se lo emplea muy frecuente para pasar con seguridad una clave privada, que posteriormente, será la que se utilice para cifrar y/o descifrar otra información” (pp. 24-25). Dentro de la encriptación asimétrica podemos encontrar una gran variedad de sistemas de cifrado que funcionan bajo los mismos parámetros como lo es el caso de RSA, El Gamal y DSA, etc. Cabe mencionar que este tipo de cifrado, garantiza mayor seguridad que los sistemas de encriptación simétrica.

En este tipo de criptografía asimétrica, ambas llaves pueden utilizarse para cifrar o descifrar los datos. Sin embargo, este proceso solo puede hacerse entre el par de llaves correspondientes, es decir, la llave privada y la llave pública correspondiente, no obstante, el proceso depende del tipo de flujo que tenga la comunicación. (Gutiérrez Ruiz, A. D., 2022, pp. 31-32)

### **RSA:**

Mayo Vilches, J. (2021). “El sistema RSA es un sistema criptográfico asimétrico considerado uno de los métodos más seguros, su nombre se debe a las siglas de sus tres fundadores (Rivest, Shamir y Adleman)” (p. 18).



Cabrera Serrano, X. A. (2023). RSA. Acrónimo de Rivest, Shamor y Adleman, apellidos de los matemáticos que definieron por primera vez este algoritmo y fue el primer algoritmo de cifrado asimétrico ampliamente disponible. Este algoritmo es conocido por la longitud de su clave y su amplio uso para la transferencia segura de datos. (P. 10)

“El sistema RSA, es considerado el primer algoritmo publicado científicamente que permite la transferencia de datos cifrados sin intercambio de claves privadas” (Mayo Vilches, J, 2021, p. 18).

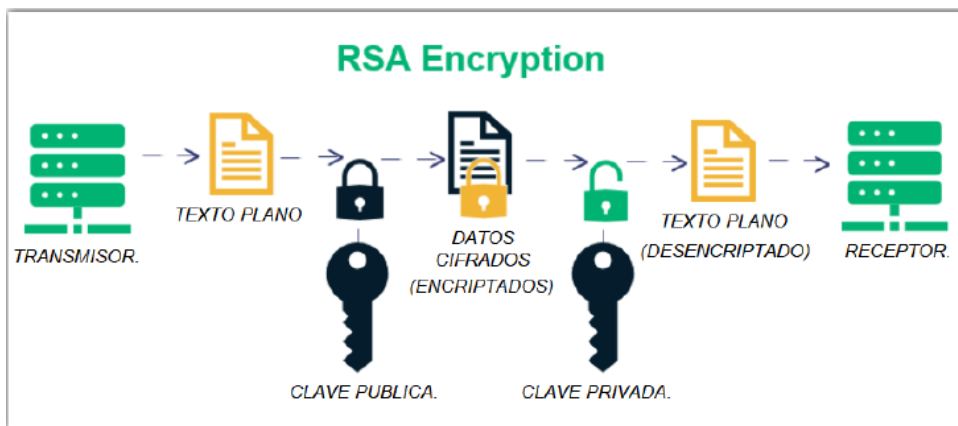


Ilustración 1. Sistema Criptográfico RSA

Fuente: Mayo Vilches, J. (2021).

### **EIGamal:**

Hasta el momento el algoritmo de cifrado EIGamal, puede ser considerado como un algoritmo efectivo. Sin embargo, si en algún momento

se puede calcular logaritmos discretos con rapidez será más o menos sencillo romper un cifrado ElGamal. Como, por el contrario, hasta la actualidad no existen algoritmos suficientemente eficientes para realizar estos cálculos en un tiempo razonable, ElGamal será un método seguro hasta que se evolucionen los ordenadores cuánticos o se cree un algoritmo efectivo, será en este momento en el que ElGamal dejará de ser un buen método de cifrado. (Pablo Sánchez, 2020, p. 8)

“El manejo de las claves juega un papel fundamental, se deben generar de una manera aleatoria. Al respecto, en criptografía asimétrica, es el propio algoritmo que genera las claves para el proceso de cifrado descifrado” (p. 45).

Lo más común es generar las claves de manera automática debido a que son más seguras, estas claves se crean y destruyen de manera automática, su durabilidad es por tiempo limitado, segundos o milésimas de segundos, algunos protocolos de comunicación las utilizan para el intercambio de información a través de un canal inseguro, ofrecen la posibilidad de cifrar el medio de transporte, en algunos casos, cifrar el contenido o mensaje que viaja por el canal. Hernández, 2018, p. 46)

### **DSA:**

Cabrera Serrano, X. A. (2023) este algoritmo asimétrico es ampliamente utilizado como algoritmo de firma digital. Está disponible en todas las librerías

criptográficas existentes como OpenSSL, GnuTLS o LibreSSL. Por lo general, no se usa para el cifrado de datos, sino solo para firmas digitales. DSA se usa más comúnmente en SSH (autenticación de servidor) que el popular RSA. (P. 10)

Traducido al español significa algoritmo de firma digital perteneciente al grupo de la criptografía asimétrica o de clave pública. Únicamente puede ser utilizado para firmas digitales, permite verificar la autenticidad de un mensaje dada la clave pública y la firma del mensaje, también se pueden generar pares de claves una pública y otra privada y generar firmas de datos utilizando la llave privada generada. (Serrato Losada, H. D., 2019, p.32).

### **Análisis del mecanismo de encriptación RCA:**

Yotam Harchol, et al. (2018) menciona que “la criptografía de umbral divide una clave secreta entre varios servidores, de modo que se requiere un número umbral de servidores para calcular operaciones criptográficas, y un número menor de servidores no aprende nada sobre la clave” (p. 23). Además, agrega que:

Sin embargo, estas construcciones requieren que todos los servidores de claves participen en cada firma. Si un servidor de claves no participa en el cálculo de una firma, su clave compartida se reconstruye y se expone a todos los demás servidores. Esta restricción es un problema importante de vida y es inaceptable en cualquier sistema a gran escala. (Yotam Harchol, et al, 2018, p. 23)

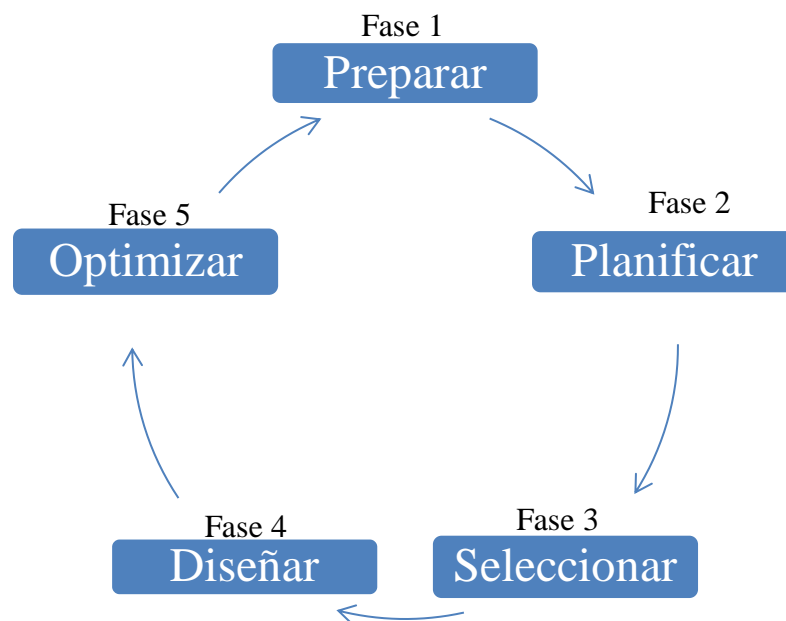
### **Análisis comparativo de mecanismos asimétricos RCA y ElGamal.**

Publicaron en la revista de sistemas computacionales Tics una comparación de dos de los algoritmos asimétricos más conocidos, su comparación se basa en realizar los procesos de cifrado y descifrado con diferentes tipos y tamaños de archivo (txt, pdf, doc, xls) y con varias longitudes de clave en bit. (Serrato Losada, H. D., 2019, p. 24) como resultado de este análisis comparativo permitieron observar que al utilizar el algoritmo RSA el archivo encriptado aumenta su tamaño hasta un 400%, y el algoritmo ElGamal hasta un 1800%, sin embargo, este último es más veloz en el proceso de cifrado.

# CAPÍTULO 2

## 2.1. Metodología

En el presente proyecto que comprende el trabajo de fin de maestría se desarrolló el tipo de investigación aplicada de corte exploratorio. La metodología utilizada para el desarrollo del proyecto comprende la siguiente estructura: Preparar, Planificar, Evaluar, Diseñar, Optimizar (PPSDO). Estas cinco fases se realizaron de forma secuencial.



*Ilustración 2: Metodología PPSDO.*

Fuente: Elaborado por el autor del proyecto.

### **FASE 1: PREPARAR.**

Se realizó el levantamiento de información de la infraestructura y los componentes del departamento de servidores, de la ISP In.Planet S.A., que se monitoreará.

## **FASE 2: PLANIFICAR.**

Dentro de esta fase, se efectuó el levantamiento de información de las necesidades en el departamento de servidores respecto a la seguridad de la información y en el que se implementará medidas de seguridad mediante mecanismos de encriptación asimétricos para salvaguardar la integridad de la información manejada en este espacio.

## **FASE 3: SELECCIONAR.**

En esta fase se procedió a la selección del mecanismo de encriptación asimétrico que cumplía con los requisitos para la implementación de las medidas de seguridad que el departamento de servidores solicitó. La selección del mecanismo de encriptación se evaluó mediante una comparativa sobre las especificidades que brindan cada uno los mecanismos de encriptación contemplados para la implementación de medidas de seguridad de la información.

## **FASE 4: DISEÑAR.**

Posterior a la selección, mediante la respectiva evaluación, se escogió el mecanismo de encriptación más adecuado para dar solución a las necesidades del departamento de servidores, de la misma manera, se procedió a diseñar de forma esquemática la arquitectura de las pertinentes medidas de seguridad dentro del departamento de servidores de InPlanet S.A., para la propuesta implementación.

## **FASE 5: OPTIMIZAR.**

Se realizó optimizaciones como una estrategia de contingencia que servirá de complemento para las medidas de seguridad brindadas por el mecanismo de

encriptación asimétrico, el cual fue contemplado para asegurar la información del departamento de servidores de InPlanet S. A., ubicado en la ciudad de Milagro.

## CAPÍTULO 3

### 3.1. Propuesta de solución

En el presente capítulo abordaremos a detalle las cinco fases que comprende este proyecto. Se levantó la información correspondiente para el *deploy*<sup>3</sup>, lo cual incluyó el inventario de infraestructura del departamento de servidores ubicado en la central Hey! Milagro de In.Planet S. A; calles Malecón 312 y Federico Proaño, del propietario Sr. Harlington René Mora Gavilánez. Posteriormente se realizó una comparativa y selección entre los principales mecanismos de cifrado asimétrico y de forma consecutiva se procedió a la implementación de la solución en un ambiente controlado. Además, se agregó una medida extra de seguridad al *RSA*<sup>4</sup>, lo cual se puede identificar en la *fase 5* que corresponde a la optimización.

### 3.2. Fase 1: Preparar.

Se realizó el levantamiento de información de la infraestructura y los componentes del departamento de servidores, de la ISP (Proveedor de Servicios de Internet) In.Planet S.A., que se monitoreará.

#### 3.2.1. Departamento de servidores:

El departamento de servidores, al cual se encuentra dirigido la implementación de las medidas de seguridad por mecanismos de encriptación asimétrico, se encuentra ubicado en la ciudad de Milagro, Malecón 312 y Federico Proaño, ¡en el edificio “HEY!”. El departamento se encuentra equipado con 12

---

<sup>3</sup> Despliegue del proyecto.

<sup>4</sup> Sistema de encriptación asimétrico fundado por Rivest, Shamir y Adleman (RSA).



servidores físicos los cuales funcionan mediante el sistema operativo CentOS, Debian y Ubuntu. Las características de cada equipo de servidores se encuentran detallada en la tabla 1.

Modelo	Nomenclatura	RAM	Disco duro	Procesador	Tamaño	Cantidad
Supermicro	ESXI 01 – 06	32 GB	2 TB	Intel Xeon E5 2.6 GHZ	1 R	6
DELL	ESXI 07 – 10	64 GB	4 TB	Xeon Silver 3.6 GHZ	2 UR	4
HP	ESXI 11 – 12	8 GB	1 TB	Xeon 2.6GHZ	E3 4 UR	2

*Tabla 1: Características generales de servidores.*

Fuente: Elaborado por el autor del proyecto.

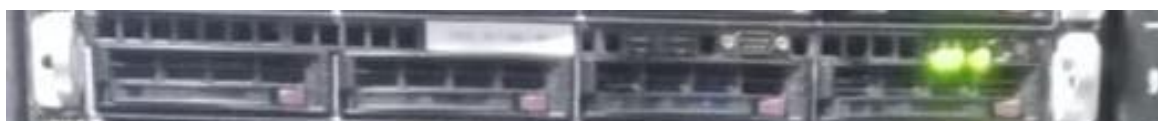
A continuación se observa las ilustraciones 3 hasta la 14 que evidencian a los servidores que comprende el departamento de servidores de la ISP In.Planet S. A. mismos que se encuentran en la tabla 1: Características de servidores.



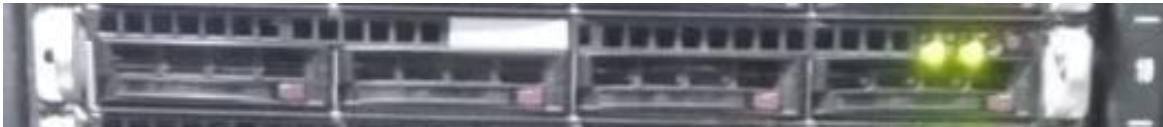
*Ilustración 3: Servidor Supermicro ESXI 01*



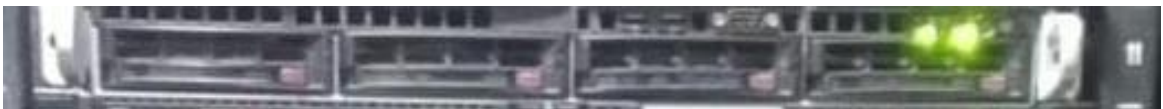
*Ilustración 4: Servidor Supermicro ESXI 02*



*Ilustración 5: Servidor Supermicro ESXI 03*



*Ilustración 6: Servidor Supermicro ESXI 04*



*Ilustración 7: Servidor Supermicro ESXI 05*



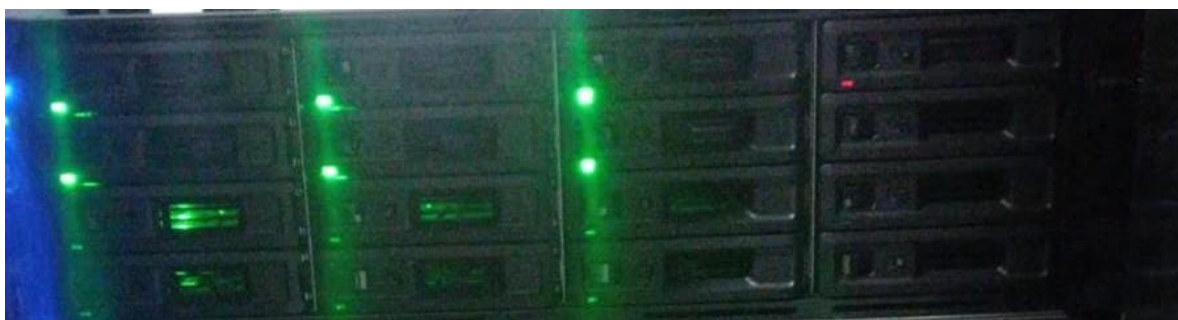
*Ilustración 8: Servidor Supermicro ESXI 06*



*Ilustración 9: Servidor DELL ESXI 7*



*Ilustración 10: Servidor DELL ESXI 8*



*Ilustración 11: Servidor DELL ESXI 9*



*Ilustración 12: Servidor DELL ESXI 10*



*Ilustración 13: Servidor HP ESXI 11*

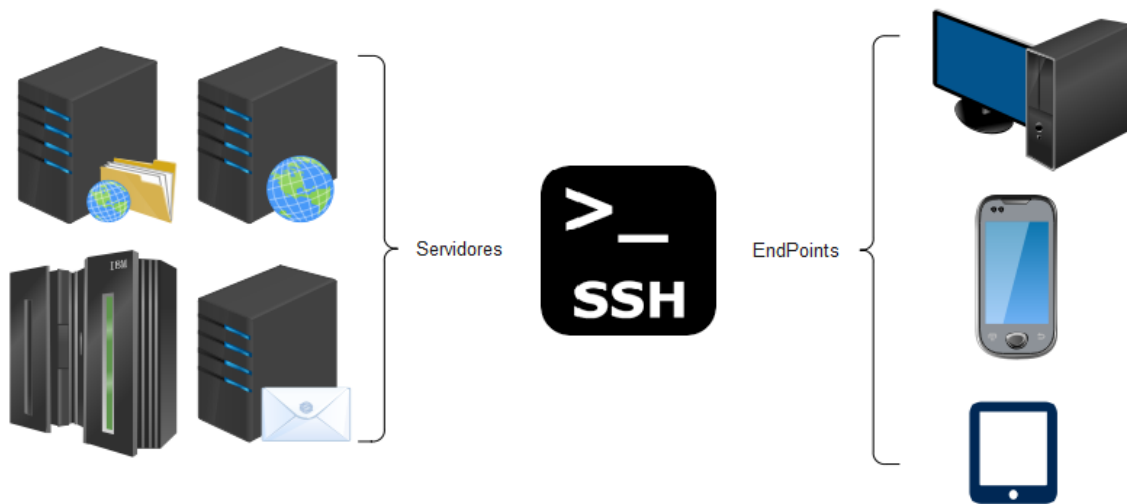


*Ilustración 14: Servidor HP ESXI 12*

### **3.2.2. Dispositivos de enlace a los servidores.**

Para ingresar a los servidores se usa un dispositivo electrónico, sea este una PC, Tablet o un smartphone. Además, requiere de una conexión mediante el

uso del protocolo SSH<sup>5</sup> un usuario y clave respectiva, como lo pueden observar en la *ilustración 15*.



*Ilustración 15: Dispositivos de enlace a los servidores.*

Fuente: Elaborado por el autor del proyecto.

### **3.2.3. Encargado del departamento de servidores.**

El técnico DataCenter Software dentro de In.Planet S.A., tiene como tarea fundamental la administración e implementación de soluciones de software libre para los servicios de red de la empresa. Dentro de los servicios que administra podemos indicar; servicio de mail Google Workspace, sistema de monitoreo CCTV, administración de la plataforma de monitoreo de red, administrar los servidores Vmware Esxi, administración y asignación de extensión en la central telefónica, administración de los respaldos de VM (Máquinas virtuales) y BD (base de datos), entre otros servicios. *En la tabla 2* se puede verificar las funciones que realiza el encargado del departamento de servidores.

---

<sup>5</sup>SSH o Secure Shell, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet mediante un mecanismo de autenticación.

<b>Cargo del encargado del departamento de servidores</b>	<b>Funciones realizadas</b>
Técnico DataCenter Software	Administra e implementa soluciones de software libre para servicios de red. <ul style="list-style-type: none"> <li>– servicio de mail Google Workspace.</li> <li>– sistema de monitoreo CCTV.</li> <li>– administración de la plataforma de monitoreo de red.</li> <li>– administrar los servidores Vmware Esxi.</li> <li>– administración y asignación de extensión en la central telefónica.</li> <li>– administración de los respaldos de VM y BD</li> </ul>

*Tabla 2: Funciones del Técnico DataCenter Software del departamento de servidores de In.Planet S.A.*

Fuente: Elaborado por el autor del proyecto.

3

### **3.2.4. Análisis económico**

La implementación de este proyecto no requiere de gastos en materiales debido a que el departamento de servidores de la ISP In.Planet S.A nos facilita de forma gratuita. Sin embargo, se debe tener en cuenta el coste de las horas de trabajo en la implementación del mecanismo de encriptación asimétrica.

Dentro del análisis financiero se constataron dos Item:

- La generación de llaves ssh
- El despliegue de las llaves ssh en los servidores de la empresa.

En la tabla 3, se detalla valores tomando en cuenta el salario que nos fue proporcionado por el técnico datacenter software, no se toman en cuenta costos por licenciamiento ya que toda la solución está implementada bajo un modelo open

source(código abierto) y free software(software gratuito).

<b>Tiempo Implementado</b>	<b>Descripción de la actividad realizada</b>	<b>Encargado</b>	<b>Precio por hora</b>
5 minutos	Generar llave SSH con mecanismo de encriptación.	Técnico DataCenter Software	0.27 dólares
5 horas	Replicación de llave SSH en los servidores	Técnico DataCenter Software	3.13 dólares
<b>Total</b>			<b>15.92 dólares</b>

*Tabla 3: Costos del tiempo de implementación basado en las horas laborales del Técnico DataCenter Software.*

### **3.3. Fase 2: Planificar.**

Dentro de esta fase, se efectuó el levantamiento de información de las necesidades en el departamento de servidores respecto a la seguridad de la información y en el que se implementará medidas de seguridad mediante mecanismos de encriptación asimétricos para salvaguardar la integridad de la información manejada en este espacio.

#### **3.3.1. Necesidades para cada equipo:**

In.Planet S.A. tiene desplegados actualmente 12 servidores físicos que ejecutan un Hipervisor de nivel 1; VMWare ESXI v7.0, los cuales manejan su nomenclatura desde el ESXI01 hasta ESXI12; dentro de estos equipos se manejan

varias máquinas virtuales (MV<sup>6</sup>), las cuales se detalla en las *tabla 4, 5 y 6*.

<b>Nomenclatura Servidores Supermicro.</b>	<b>Máquinas Virtuales por servidor.</b>	<b>Especificidades Sistemas operativos que utilizan las MV.</b>
ESXI01	3 VM	2 VM Ubuntu 1 VM CentOS
ESXI02	2 VM	2 VM Ubuntu
ESXI03	2 VM	1 VM Ubuntu 1 VM Debian
ESXI04	6 VM	5 VM Debian 1 VM Windows (no aplica al proyecto)
ESXI05	8 VM	6 VM Ubuntu 2 VM CentOS
ESXI06	5 VM	1 VM Ubuntu 3 VM CentOS 1 VM Debian

*Tabla 4: Servidores Supermicro y sus respectivas Máquinas Virtuales a las cuales se aplicará el respectivo mecanismo de encriptación asimétrico.*

Fuente: Elaborado por el autor del proyecto.

<b>Nomenclatura Servidores DELL.</b>	<b>Máquinas Virtuales por servidor.</b>	<b>Especificidades Sistemas operativos que utilizan las MV.</b>
ESXI07	8 VM	3 VM CentOS 5 VM Ubuntu
ESXI08	7 VM	4 VM Ubuntu 3 VM Windows (no aplica al proyecto)
ESXI09	8 VM	7 VM Ubuntu 1 VM CentOS
ESXI10	2 VM	2 VM Ubuntu

<sup>6</sup> Máquinas virtuales.

*Tabla 5: Servidores DELL y sus respectivas Máquinas Virtuales a las cuales se aplicará el respectivo mecanismo de encriptación asimétrico.*

Fuente: Elaborado por el autor del proyecto.

<b>Nomenclatura Servidores HP.</b>	<b>Máquinas Virtuales por servidor.</b>	<b>Especificidades Sistemas operativos que utilizan las MV.</b>
ESXI11	5 VM	4 VM Ubuntu 1 VM Debian
ESXI12	4 VM	3 VM CentOS 1 VM Debian

*Tabla 6: Servidores HP y sus respectivas Máquinas Virtuales a las cuales se aplicará el respectivo mecanismo de encriptación asimétrico.*

Fuente: Elaborado por el autor del proyecto.

### **3.3.2. Especificidades de requerimientos solicitados:**

Se realizó el correspondiente levantamiento de información al departamento de servidores en el cual se identificó cuatro requerimientos; mayor seguridad SSH, soporte, implementación y administración. Se requiere *mayor seguridad SSH*, debido a que actualmente se han encontrado fallos de seguridad en el protocolo. En el caso de *soporte*, las medidas a implementar deben estar relacionados en todos los sistemas operativos que tiene ejecutando la empresa. De la misma manera, *la implementación* de la solución debe ser sencilla de implementar para personal técnico de la empresa. Por último, en relación a la *administración*, la medida de seguridad a implementar deberá enlazar con los distintos dispositivos que posea el administrador para ingresar a la información requerida. La prioridad de los requerimientos se puede evidenciar en la *tabla 7 Análisis de necesidades del departamento de servidores*.



<b>Requerimiento</b>	<b>Descripción</b>	<b>Prioridad</b>
Mayor seguridad SSH	La solución y la encriptación deberán aportar una seguridad robusta	Alta
Soporte	La solución y la encriptación deberán ser compatibles con las distribuciones Linux, CentOS, Ubuntu y Debian	Alta
Implementación	La solución y la encriptación deben ser de fácil implementación para el personal técnico	Alta
Administración	La solución debe poder ser usada en todos los dispositivos que el admin utiliza, sean estos PC, Tablet, smartphone, laptop.	Alta

*Tabla 7: Análisis de necesidades del departamento de servidores.*

Fuente: Elaborado por el autor del proyecto.

### **3.4. Fase 3: Seleccionar.**

En esta fase se procedió a la selección del mecanismo de encriptación asimétrico que cumplía con los requisitos para la implementación de las medidas de seguridad que el departamento de servidores solicitó. La selección del mecanismo de encriptación se evaluó mediante una comparativa sobre las especificidades que brindan cada uno los mecanismos de encriptación contemplados para la implementación de medidas de seguridad de la información.

### 3.4.1. Características y comparación entre RSA, DSA y ElGamal.

Se realizó una comparativa de las principales características de los mecanismos de encriptación a analizar, mediante la cual se logró contrastar la información descrita en la *tabla 8*. Se realizó una comparativa nos permitió elegir de forma más precisa el mecanismo de encriptación a usar en la implementación de la solución. Además, se procedió a evaluar los mecanismos de encriptación lo cual se puede observar en la *tabla 9: Evaluación de los mecanismos de encriptación asimétricos RSA, DSA y ElGamal*.

<b>Característica</b>	<b>RSA</b>	<b>DSA</b>	<b>ElGamal</b>
<b>Tipo de algoritmo:</b>	Cifrado y firma	Firma digital	Cifrado y firma
<b>Seguridad:</b>	Seguro si se usa con claves largas (2048 bits o más)	Seguro para firmas digitales	Seguro si se usa con claves largas (2048 bits o más)
<b>Generación de claves:</b>	Generación de claves largas es más lenta, pero más segura	Generación de claves más rápida	Generación de claves largas es más lenta
<b>Tamaño de clave típico:</b>	2048 bits o más.	2048 bits o más.	2048 bits o más.
<b>Uso típico:</b>	Comunicaciones seguras, firmas digitales.	Firmas digitales en autenticación.	Comunicaciones seguras, firmas digitales.
<b>Fortaleza matemática:</b>	Basado en la factorización de números primos.	Basado en el problema del logaritmo discreto.	Basado en el problema del logaritmo discreto.
<b>Rendimiento:</b>	Cifrado y descifrado más	Rápido en generación de	Cifrado y descifrado más

	lento que DSA, firmas digitales. pero más seguro.		lento que DSA.
<b>Patente:</b>	No patentado.	No patentado.	No patentado.
<b>Vulnerabilidades:</b>	Vulnerable si se utilizan claves cortas o se encuentra una factorización eficiente.	Vulnerable si no se manejan adecuadamente las claves.	Vulnerable si se utilizan claves cortas o se encuentra una factorización eficiente.

*Tabla 8: comparativa de características entre los mecanismos de encriptación asimétrica RSA, DSA y ElGamal.*

Fuente: Elaborado por el autor del proyecto.

### **3.4.2. Evaluación de los mecanismos de encriptación asimétricos para la aplicación para las medidas de seguridad del departamento de servidores.**

Posteriormente a la comparativa realizada en los tres mecanismos de encriptación asimétrica, se realizó la evaluación y la correspondiente selección del mecanismo a utilizar. Como resultado de dicha evaluación, el mecanismo de encriptación asimétrico RSA resultó cumplir con los parámetros necesarios que requiere el departamento de servidores para mejorar la seguridad de la información que se maneja en el departamento. Véase la *tabla 9 Evaluación de los mecanismos de encriptación asimétricos RSA, DSA y ElGamal.*

Requerimiento	Descripción	Prioridad	RSA	DSA	EIGamal
Mayor seguridad SSH	La solución y la encriptación deberán aportar una seguridad robusta	Alta	✓	✓	✓
Soporte	La solución y la encriptación deberán ser compatibles con las distribuciones Linux, CentOS, Ubuntu y Debian	Alta	✓	✓	✓
Implementación	La solución y la encriptación deben ser de fácil implementación para el personal técnico	Alta	✓	X	X
Administración	La solución debe poder ser usada en todos los dispositivos que el admin utiliza, sean estos PC, Tablet, smartphone, laptop.	Alta	✓	✓	X

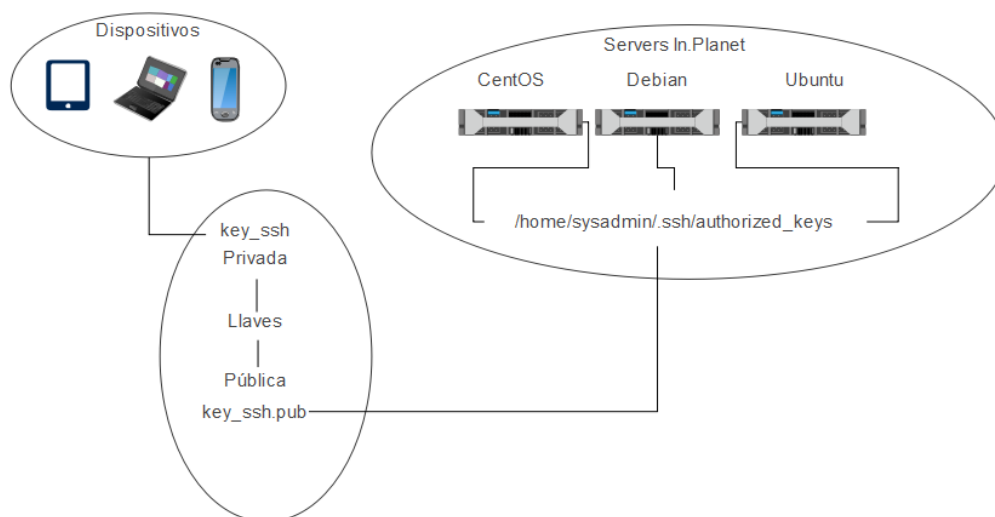
*Tabla 9: Evaluación de los mecanismos de encriptación asimétricos RSA, DSA y EIGamal.*

Fuente: Elaborado por el autor del proyecto.

### 3.5. Fase 4: Diseñar.

Posterior a la selección, mediante la respectiva evaluación, se escogió el mecanismo de encriptación más adecuado para dar solución a las necesidades del departamento de servidores, de la misma manera, se procedió a diseñar de forma esquemática la arquitectura de las pertinentes medidas de seguridad dentro del departamento de servidores de InPlanet S.A., para la propuesta implementación.

#### 3.5.1. Arquitectura del funcionamiento del mecanismo de encriptación



*Ilustración 16: Diseño de la arquitectura de la propuesta de solución.*

*Fuente: Elaborada por el autor del proyecto.*

Para la creación de la llave se usó el sistema operativo Windows 11, sin embargo, los mismos pasos usados en dicho sistema para la generación de la llave ssh (secure Shell) pueden ser usados en una distribución Linux Desktop.

El primer paso que se realizó fue la creación del par de llaves, para lo cual se usó el comando `ssh-keygen` (como puede observar en la ilustración 17), el tipo de encriptación usada fue RSA (Rivest, Shamir y Adleman) con una longitud de 4096

bits (como se puede corroborar en la Ilustración 18).

```
C:\Users\SysAdmin>ssh-keygen -t rsa -b 4096
```

*Ilustración 17: Comando para genera las de llaves SSH; privada y pública.*

```
C:\Users\SysAdmin>ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\SysAdmin/.ssh/id_rsa):
```

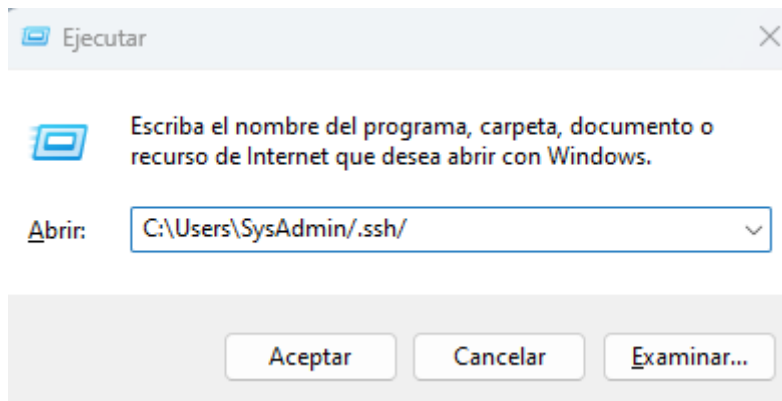
*Ilustración 18: Pedirá que se les dé un nombre a los archivos en caso de dejarlo por defecto se dará enter y se guardaran como id\_rsa.*

Como medida adicional se seguridad se configuró una contraseña para la llave SSH (Secure Shell/Shell Segura), la cual como recomendación debe ser muy diferente a la contraseña que usa el administrador del servidor. Una vez todo el proceso se cumplió se podrá observar el fingerprint (huella digital) de la llave SSH (Secure Shell/Shell Segura). El resultado lo pueden observar en la *ilustración 20*.

```
C:\Users\SysAdmin>ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\SysAdmin/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\SysAdmin/.ssh/id_rsa
Your public key has been saved in C:\Users\SysAdmin/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:AGfpcns3j2tZBqnyPE2G0YJbizu8Pr9hW0U3Yii5F+o sysadmin@DESKTOP-IAQ9H7M
The key's randomart image is:
+----[RSA 4096]-----+
|  . 0 . |
| +.. . |
| 0+.0 +.0 |
| 0 *+.+00 . |
| *0*S... |
| 0=-.*.0 0 |
| .EX.. B |
| =..+0 + . |
| .0=+. ... |
+----[SHA256]-----+
C:\Users\SysAdmin>
```

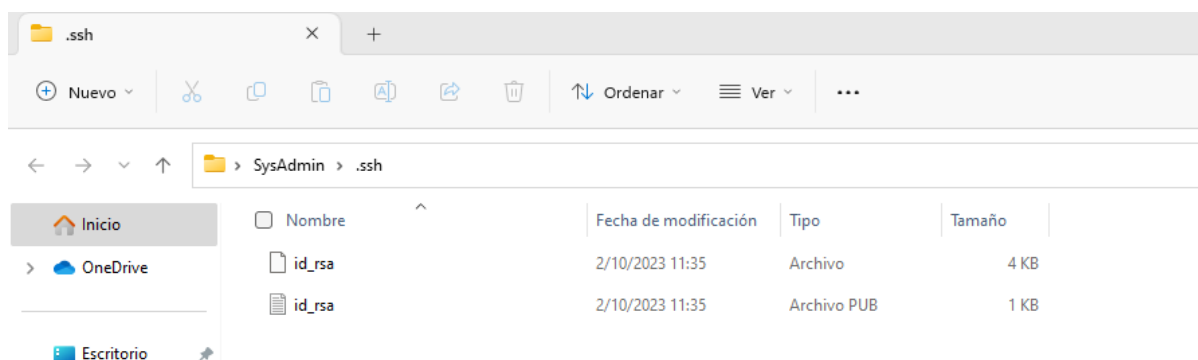
*Ilustración 19: La llave fue generada con éxito.*

La llave ssh fue creada con éxito en la dirección predeterminada del sistema operativo la cual es “C:\Users\SysAdmin/.ssh/”, para llegar a esta ubicación se usó la herramienta Ejecutar del sistema operativo Windows para acceder a la información como se puede corroborar en la *ilustración 21*.



*Ilustración 20: Nos ubicaremos en el directorio donde se alojan las llaves SSH creadas.*

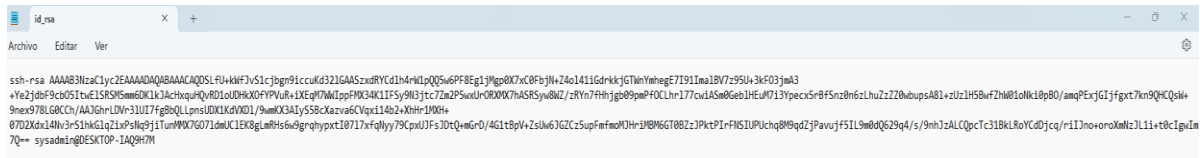
Encontraremos dos archivos un sin tipo y uno de formato PUB el cual es la llave publica que se configura en los equipos remotos. Los dos archivos creados (el par de llaves) 2corresponden a id\_rsa como la llave privada y id\_rsa.pub como la llave pública. Véase la *ilustración 22*.



*Ilustración 21: llave privada id\_rsa y llave pública id\_rsa.pub*

Se comprobó el contenido de la llave publica, usando la aplicación Notepad del sistema operativo Linux, en el cual podremos observar un conjunto de caracteres que

pueden no tener sentido, pero componen la llave pública. En la ilustración 23 se puede observar el contenido de la llave pública.

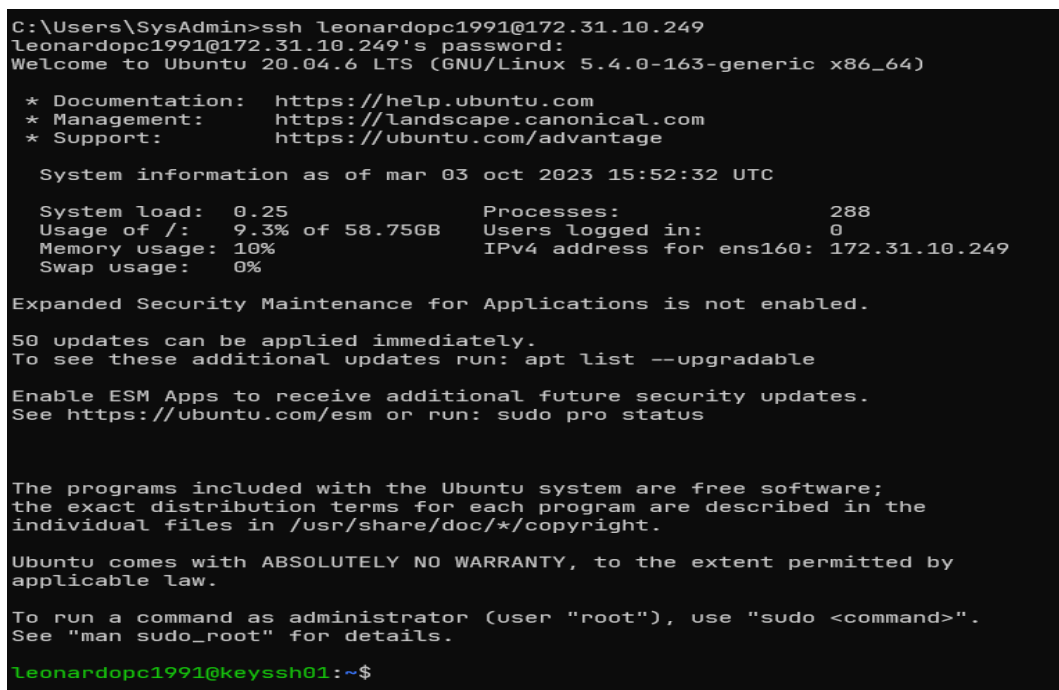


```
id_rsa
Archivo  Editar  Ver

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCSlFvKkF7vS1c3jgng9iccuKd321GAASxdRyCd1h4nM1pQ05w6PF8Eg1j9ep8X7c0Fb7jH+Z4o1411GdrkKjG7lnYmhegE71911ma1Bw7z95U+3kF03jml3
+YeZjdbF9cb051twE1SR9M6m6DK1kAChkquq0uRD1oUHkXOPFVUuR+1XEgM7M1ppF9034K11F5y9N3jtc7z2P5x0r0R0X7hASRSyW8WZ/zRYn7Fhng09pmPFOCLhr177cvdASm0GebIHEu0713Ypecx5rBf5nz0b6zLhuZzZ2b0upsA81+zUzIh5BwF7hW010k10p80/amqPExjGijfgxt7kn9qKQsW+
9mex978L68Cch/AAJGhrLDVr31U17f7g8QLlpsU0K1Kv0D1/9am0K3AlY558Ckzva6Cvq140z+Xkhr1MWH+
070ZK6v14hV3rS1M6lqzLp9hg9j1TurM9K7G0710m0C1EK8gUm9S6w9grqhyptx10711xfqly79CpxUJFsJ0tQmGr0/4G1t8pV+ZsUw6J2Cz5upFmf0UHr3M8M6T08Zz3PktPIrFHSIUUchq8B9qdz3PavujF5119m00Q629q4/s/9nh1zALC0pcTc31BkLR0YCdJcj/r111no+oroMmZ3L11+0c1GvIm
7Q== sysadmin@ESKTOP-1A9H7H
```

Ilustración 22: Si se abre el archivo podremos ver el contenido de la llave.

Se procedió a configurar el sistema operativo que usará la llave pública, el cual es un Ubuntu (esta misma configuración funciona tanto en sistemas Debian y CentOS) para lograr esta configuración iniciaremos sesión mediante el protocolo SSH (secure shell) de manera tradicional es decir con un usuario y contraseña. El sistema Ubuntu que fue instalado para este ambiente controlado tiene por IP 172.31.10.249, la cadena de conexión es ssh usuario@ip\_servidor, para este caso la conexión fue SSH leonardopc1991@172.31.10.249, así como se puede identificar en la ilustración 24.



```
C:\Users\SysAdmin>ssh leonardopc1991@172.31.10.249
leonardopc1991@172.31.10.249's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-163-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of mar 03 oct 2023 15:52:32 UTC

System load:  0.25          Processes:    288
Usage of /:   9.3% of 58.75GB Users logged in: 0
Memory usage: 10%          IPv4 address for ens160: 172.31.10.249
Swap usage:  0%

Expanded Security Maintenance for Applications is not enabled.

50 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

leonardopc1991@keyssh01:~$
```

Ilustración 23: Ingreso al servidor para configurar las llaves y el servicio OpenSSH.



Una vez que se logró conectarse al servidor remoto, se procedió a elevar privilegios a nuestro usuario esto se logró con el comando `sudo -i` donde acto seguido nos pidió que ingresemos nuestra contraseña, luego de ingresar la clave del usuario, la terminal pasó a tener acceso de root como lo muestra la ilustración 25.

```
leonardopc1991@keyssh01:~$ sudo -i  
[sudo] password for leonardopc1991  
root@keyssh01:~#
```

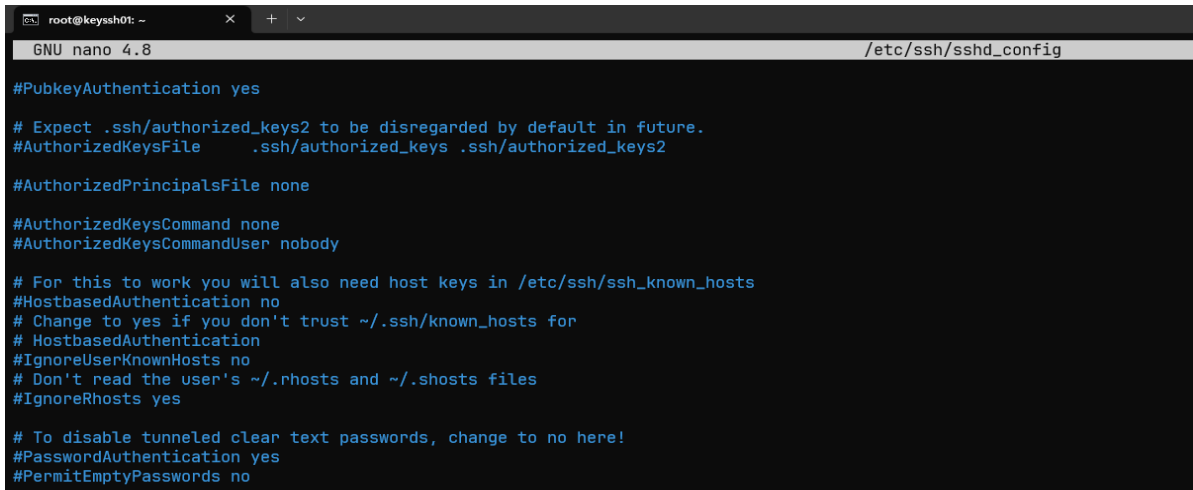
*Ilustración 24: Otorgar permisos de root al usuario.*

Se procedió a configurar el servicio ssh(secure Shell) para que solo permita la conexión mediante el uso de llaves y mas no con usuario y contraseñas que es el método de acceso común. Para realizar esta actividad se editó el archivo de configuración `sshd_config`, que está ubicado en la ruta `/etc/ssh`, este fichero fue actualizado usando el editor de archivos nano. Véase la *ilustración 26*.

```
root@keyssh01:~# nano /etc/ssh/sshd_config
```

*Ilustración 25: Modificaremos el archivo `sshd_config`.*

Dentro del fichero se encuentran todas las configuraciones necesarias para que el servicio de ssh(secure Shell) funcionen de manera correcta, dentro del mencionado fichero(`sshd_config`) encontraremos la línea `PasswordAuthentication` la cual por defecto se encuentra comentada con el símbolo del numeral y con el parámetro `yes` como lo muestra la *ilustración 27*.



```
root@keyssh0t: ~
GNU nano 4.8 /etc/ssh/sshd_config

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

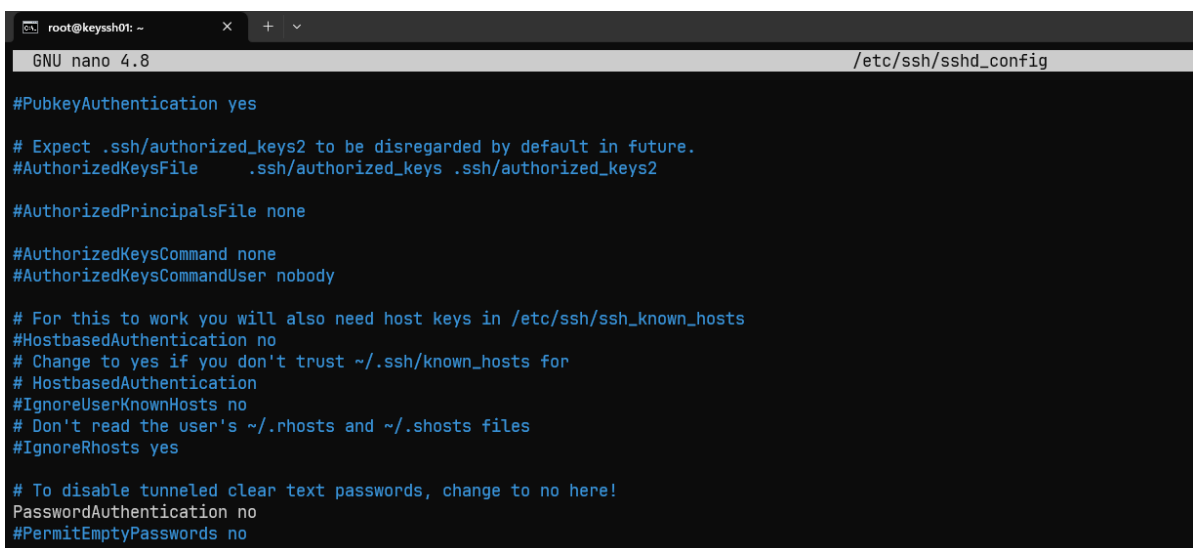
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
```

*Ilustración 26: Buscaremos la línea PasswordAuthentication que por defecto está comentada.*

Para que la conexión hacia el servidor solo permita el uso de llaves ssh (secure Shell) se quitó el numeral (se descomentó) y como parámetro se configuró no, con esta configuración se estableció que no permita el uso de contraseñas para la autenticación como se puede identificar en la *ilustración 28*.



```
root@keyssh0t: ~
GNU nano 4.8 /etc/ssh/sshd_config

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

*Ilustración 27: La descomentaremos y cambiaremos el yes por no.*

Para que los cambios surtan efecto se debió reiniciar el servicio de ssh (secure Shell) esto se logró con el comando `systemctl restart sshd`. Véase la *ilustración 29*.

```
root@keyssh01:~# systemctl restart sshd
root@keyssh01:~#
```

Ilustración 28: Reiniciaremos el servicio de SSH.

Como último paso para el deploy(despliegue o lanzamiento) de la llave ssh(secure Shell) se añadió el contenido de la llave publica en el fichero `authorized_key`, el cual, se encuentra dentro de la carpeta oculta SSH en el directorio del usuario con el que nos conectamos al servidor. La ruta de este archivo fue `/home/leonardopc1991/.ssh`, el archivo se modificó con el editor de texto nano: como se indica la ilustración 30 con la flecha color rojo.

```
root@keyssh01: /home/leona | x + v
root@keyssh01:~# cd /home/leonardopc1991/
root@keyssh01:/home/leonardopc1991# cd .ssh
root@keyssh01:/home/leonardopc1991/.ssh# ls
authorized_keys
root@keyssh01:/home/leonardopc1991/.ssh# nano authorized_keys
root@keyssh01:/home/leonardopc1991/.ssh#
```

Ilustración 29: Ingreso al directorio de llaves del usuario y modificaremos el archivo `authorized_keys`.

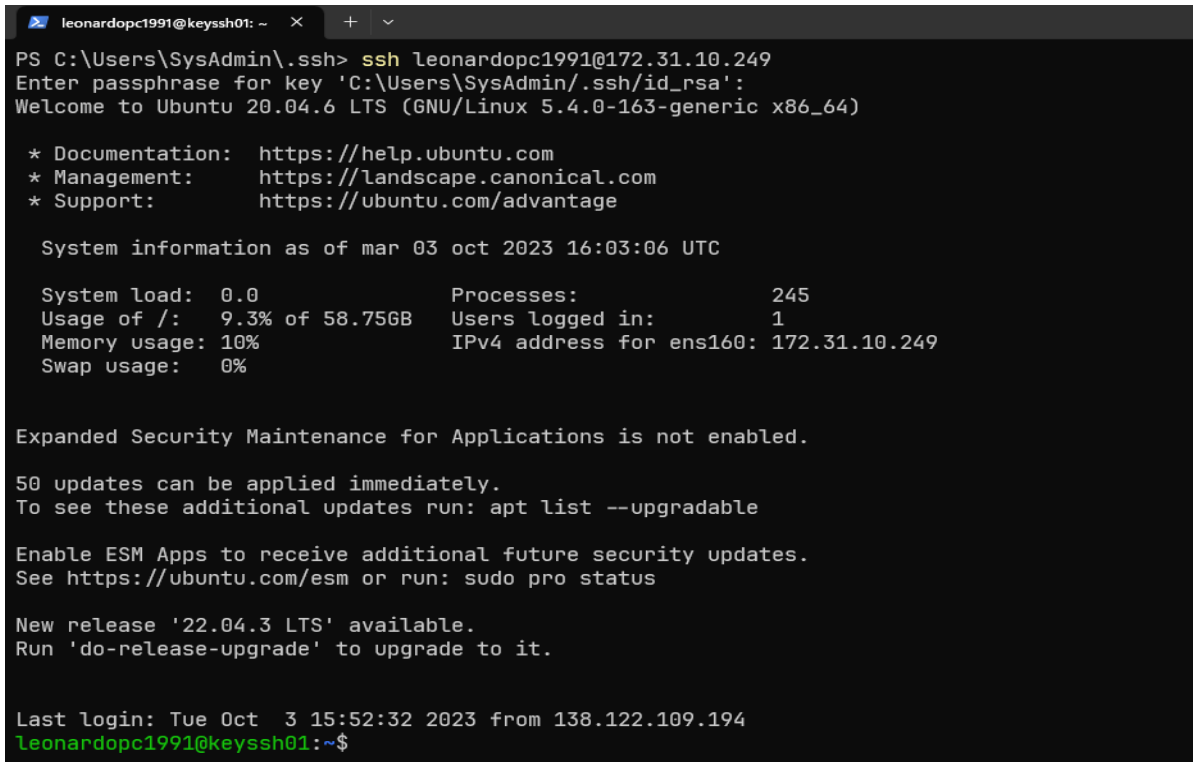
Procedimos a pegar el contenido de la llave SSH en el archivo antes mencionado, se guardó los cambios y se cerró el archivo que se encontraba modificando. En la *ilustración 31* se puede observar el contenido de la llave SSH.

```
GNU nano 4.8 authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACzE1t3zxV9X0Fsf4pE5agWHxssUKLhUSN+KEiKDfa/Upw/z93xWi1fL4AH+aejS8lWgtBLVvQZ6fhBy0n28Q8+3s8NBm18>
```

Ilustración 30: Pegaremos el contenido del archivo `id_rsa.pub` y guardaremos.

La *ilustración 32* se puede observar, cuando, una vez concluido el deploy

(despliegue o lanzamiento) de la llave ssh (Secure Shell) en el servidor de ambiente controlado, se procedió con las pruebas pertinentes para corroborar el correcto funcionamiento del mismo. Se uso el mismo formato de conexión con el cual se inicia sesión a un servidor por ssh, pero añadiendo el parámetro -i seguido de la ubicación y nombre de la llave privada.



```
leonardopc1991@keyssh01: ~ × + v
PS C:\Users\SysAdmin\.ssh> ssh leonardopc1991@172.31.10.249
Enter passphrase for key 'C:\Users\SysAdmin\.ssh/id_rsa':
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-163-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of mar 03 oct 2023 16:03:06 UTC

System load:  0.0                Processes:    245
Usage of /:   9.3% of 58.75GB     Users logged in:  1
Memory usage: 10%                IPv4 address for ens160: 172.31.10.249
Swap usage:  0%

Expanded Security Maintenance for Applications is not enabled.

50 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Oct  3 15:52:32 2023 from 138.122.109.194
leonardopc1991@keyssh01:~$
```

*Ilustración 31: Iniciaremos sesión nuevamente en el server y esta vez pedirá la clave de la llave SSH.*

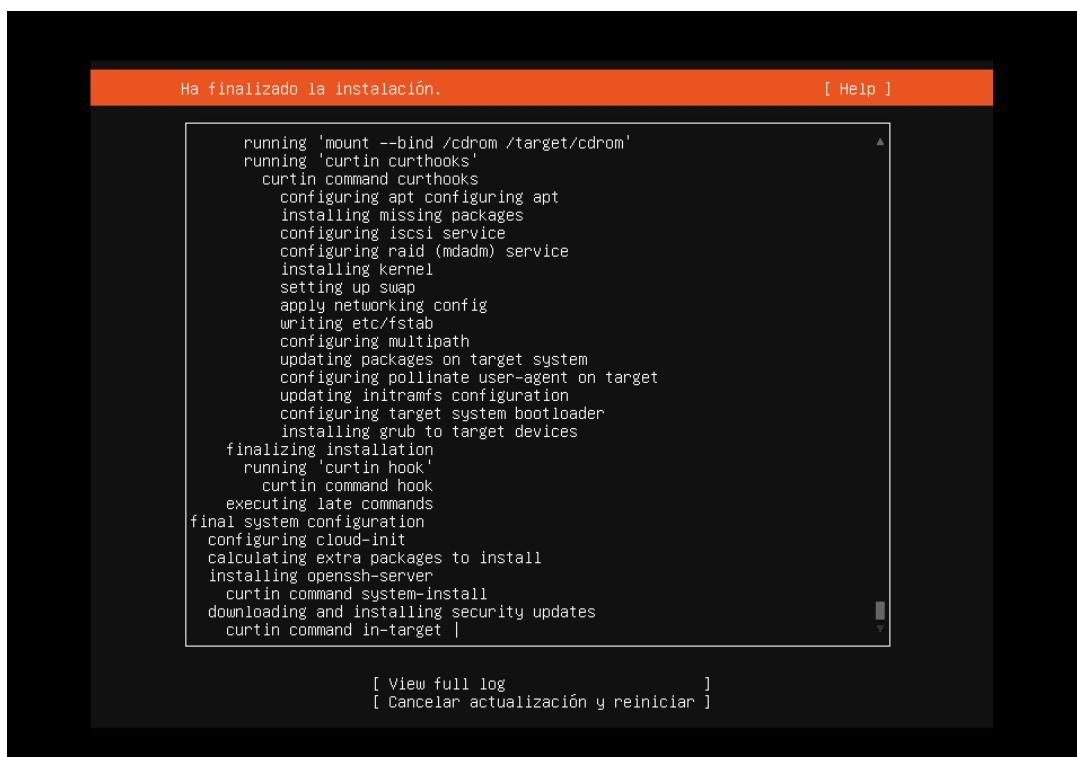
### **3.6. Fase 5: Optimizar.**

Se realizó optimizaciones como una estrategia de contingencia que servirá de complemento para las medidas de seguridad brindadas por el mecanismo de encriptación asimétrico, el cual fue contemplado para asegurar la información del departamento de servidores de InPlanet S.A.

#### **3.6.1. Capa extra de seguridad.**

La optimización se la realiza con el fin de dar una capa más de seguridad a la solución implementada, para esto se va a instalar un servidor donde se ubicará la llave de acceso al o los servidores. Adicional, en el server a administrar se añadirá reglas de firewall para que solo permita la conexión desde el servidor master.

La ilustración 34 hace referencia a que la implementación en el ambiente controlado se dio de manera correcta, sin embargo, el técnico de datacenter indico si había manera de centralizar las conexiones a los servidores desde un solo servidor, para lo cual se instaló Ubuntu Server 20.04 LTS con una ip 172.31.10.242.



```
Ha finalizado la instalación. [ Help ]

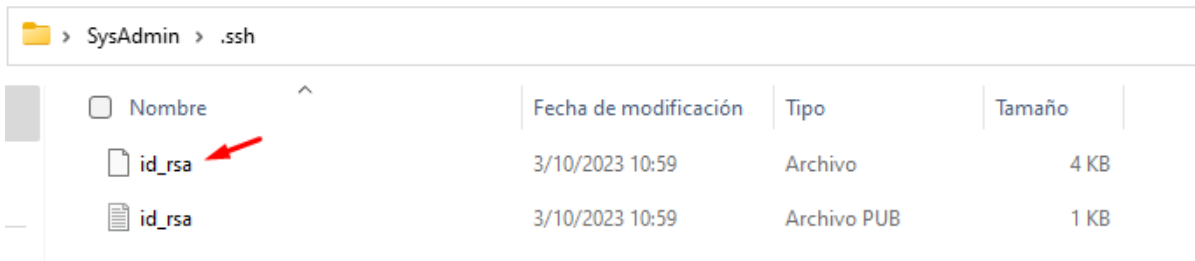
running 'mount --bind /cdrom /target/cdrom'
running 'curtin curthooks'
curtin command curthooks
  configuring apt
  configuring apt
  installing missing packages
  configuring iscsi service
  configuring raid (mdadm) service
  installing kernel
  setting up swap
  apply networking config
  writing etc/fstab
  configuring multipath
  updating packages on target system
  configuring pollinate user-agent on target
  updating initramfs configuration
  configuring target system bootloader
  installing grub to target devices
finalizing installation
running 'curtin hook'
curtin command hook
  executing late commands
final system configuration
  configuring cloud-init
  calculating extra packages to install
  installing openssh-server
curtin command system-install
  downloading and installing security updates
curtin command in-target |

[ View full log ]
[ Cancelar actualización y reiniciar ]
```

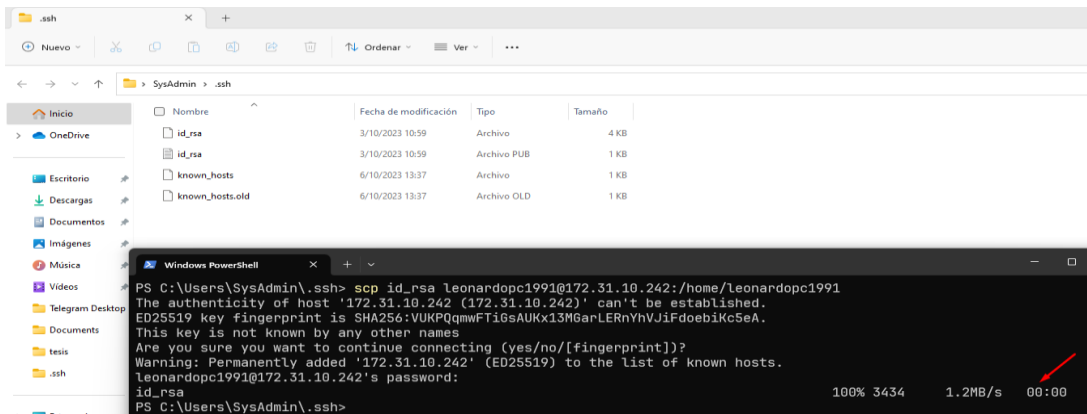
*Ilustración 32: Instalamos un nuevo servidor.*

Al no usar el dispositivo del técnico para la conexión, se debió mover la llave privada hacia el nuevo servidor, esta tarea la realizamos con el comando scp (secure copy protocol) donde se usó la cadena de conexión scp archivo

usuario@ip\_server:/directorio/a/copiar, para el caso de nuestro servidor fue scp id\_rsa leonardopc1991@172.31.10.242:/home/leonardopc1991. La *ilustración 35* y *36* se puede corroborar lo ya mencionado.



*Ilustración 33: Identificaremos la llave privada.*



*Ilustración 34: Una vez instalado el nuevo servidor copiaremos la llave privada a dicho servidor.*

Iniciamos sesión de la manera tradicional usando ssh (secure Shell), el comando que se utilizó fue ssh leonardopc1991@172.31.10.242, luego ejecutamos el comando ls, el cual nos permite listar todos los archivos o carpetas que se encuentren en el directorio donde nos encontremos. Véase la *ilustración 37*, la llave generada se encuentra señalada mediante una flecha color rojo.

```

PS C:\Users\SysAdmin> ssh leonardopc1991@172.31.10.242
leonardopc1991@172.31.10.242's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-164-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of vie 06 oct 2023 18:40:59 UTC

System load:  0.0          Processes:            230
Usage of /:   29.0% of 15.64GB  Users logged in:    0
Memory usage: 14%          IPv4 address for ens160: 172.31.10.242
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

50 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

leonardopc1991@masterssh01:~$ ls
id_rsa
leonardopc1991@masterssh01:~$

```

*Ilustración 35: La llave se copiará en la ruta indicada.*

Para tener un nombre más significativo al archivo de llave privado, se procedió a cambiar el nombre con el comando mv donde se pasó pro parámetro el nombre actual del archivo y el nombre que le dio, luego se ejecutó el comando ls y se observó el archivo de llave ssh (secure Shell) con el nombre cambiado. Véase la *ilustración 38*.

```

leonardopc1991@masterssh01:~$ mv id_rsa llave
leonardopc1991@masterssh01:~$ ls
llave
leonardopc1991@masterssh01:~$

```

*Ilustración 36: Campiaremos el nombre del archivo.*

Ejecutamos el comando cat (él nos permite ver en consola el contenido de un archivo) seguido del nombre que le dimos al fichero de la llave privada, podremos

ver el contenido, mismo que se puede identificar en la *ilustración 39*.

```
leonardopc1991@masterssh01:~$ cat llave
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABA4mAHNGi
gSf71g+c9C+TIQAAAAEAAAAEAAAIXAAAAAB3NzaC1yc2EAAAADAQABAAQACze1t3zxV9
X0Fsf4pE5agWHxssUKLhU5N+KEiKdFa/Upw/z93xWi1fL4AH+aejS8lWgtBLVvQZ6fhBy0
n28Q8+3s8NBm18gFjBV6vdjPDiHgKj2ywedkKyBZsEPtUTJ8ZYRzz+0uzdnW9dwr0cJu9L
0ftZKun+5kGnKIwxwY6E2iB0Z90JINeT8swngweFZsBPgNvA7DAYVY4MCeVXo4HTMh5wZw
LM2qjdheYKEZSzi2A/gQadnL/vz1irjGULxYCDcnuay08necbaJYxtRq+D2x7vPShlk4+J
rthiEojQnxBj/bdWRMvQkCGTL+hjZHKnkxkzhx0pAJT5B+bC0sIw50cn8Sg270NVxHiJZj
CrP7hZLN8pEsJJfYcjWHJof3w2PZcEB2ELxpBVrsRkIXhnV500nNiqJa4KFxX2EIIiTY0U
mFbfbmIPguvvdLLwAqDPQ4wiq+/66TYLCrMUDwcMPdy3zJKwuY80JSKfj7J74S/FoL0zBy9
aQCey0VNHb71Ih6E1hG1fSZIeVX/0id4E7Qhbkbczk1WBMGMNNxdxw+0DXd0z707VjJemJL
3h6LvMoG2MP0vzZPCn5vQW76a3XcS8n9Qz0zMhumprcsLsaE3EJGJbv8c5KDFvtt7JqNn
LgkflPI5qTp4RVVgAg3BfSW6NxxSsP5gLunKuh4dmw9wAAB1DV01BNG1RAuT89oF8/LXPn
798SauZyP5b4+wMSBvmI0/6JjtMZDyL5a1FiGEvEbQW5AEes9HZ7xbAIC7R80Rhiw29JVb
Gv3E3U4WzxbjZs+XtczuIz7rPSEyEY3+yV/Do0ykdw+6Y8ZyhwKxSV/BMM6Wlw0yXisaLZ
ZXNaH3pRP+xRpfRwsKnctUbyYHzW8tFS7nPkZ/2KJZY3aK6b+I10NtUx0TewDE79Vx1kZt
5ey9moex5YApElwAC1W3MZdRi0TySrExkuv0K1YaJJ/EBbzVHND3Qf66zBkTcab7LCE2KB
```

*Ilustración 37: Realización de un cat para ver el contenido de la llave privada.*

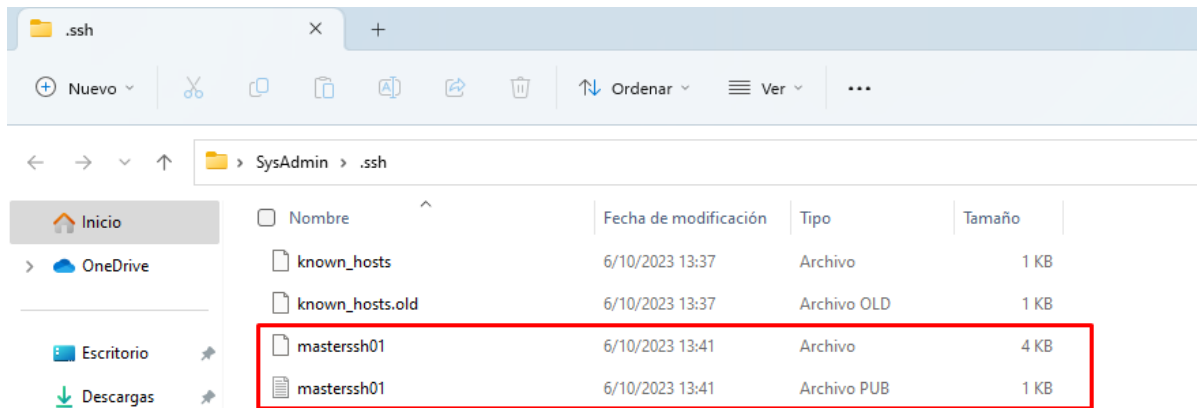
En la *ilustración 40* se muestra la generación de un nuevo par de llaves el cual permitirá la conexión al servidor centralizado de ssh (secure Shell), seguiremos el mismo proceso que fue descrito anteriormente para la creación de las llaves ssh (secure Shell) usando el sistema de encriptación RSA (Rivest, Shamir y Adleman) con una longitud de 4096 bits.

```
PS C:\Users\SysAdmin\.ssh> ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\SysAdmin\.ssh\id_rsa): masterssh01
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in masterssh01
Your public key has been saved in masterssh01.pub
The key fingerprint is:
SHA256:DVV8MSgl3KTnkDrA8xZo4dy3LmePSR+6/NRCrG2NHpE sysadmin@DESKTOP-IAQ9H7M
The key's randomart image is:
+---[RSA 4096]-----+
|
| . .0*+.0. |
| + + .0++ .. |
| 0 + =... |
| . + * * . . |
| S = = E |
| . o + X * |
| = X o |
| . = o |
| o.o |
+----[SHA256]-----+
PS C:\Users\SysAdmin\.ssh>
```

*Ilustración 38: Generar otro par de llaves que permitirá la conexión al servidor máster.*

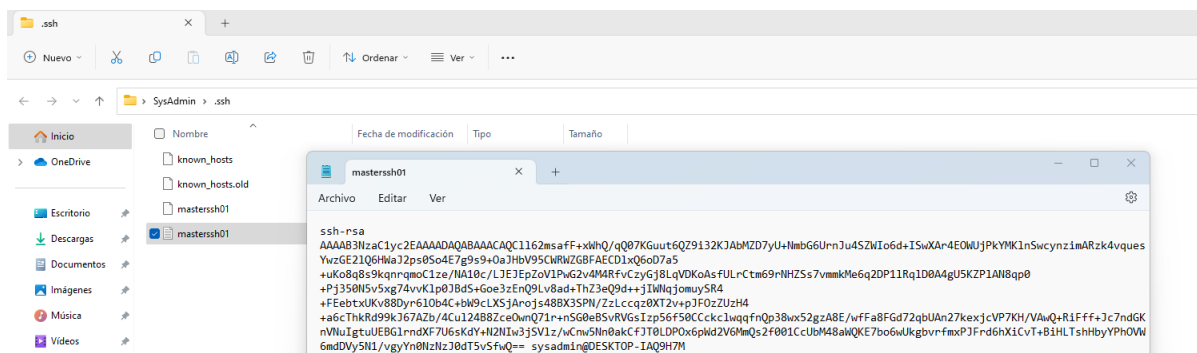


Posteriormente como se señala en la *ilustración 42*, el par de llaves fueron creadas en el directorio por defecto del sistema operativo Windows.



*Ilustración 39: Los archivos fueron creados.*

Con el editor de texto Notepad del sistema operativo Windows pudimos ver el contenido de la llave, el cual deberá ser copiado en el fichero authorized\_key del servidor. Véase la *ilustración 43*.



*Ilustración 40: Contenido de la llave pública.*

Como se puede verificar en la *ilustración 44*, iniciamos sesión en el servidor centralizado, y nos ubicaremos en la carpeta oculta de ssh (secure Shell). Con el editor de texto nano modificaremos el fichero authorized\_keys en el cual pegamos en contenido de la llave publica que anteriormente habíamos visualizado. Véase la *ilustración 45*.

```

Leonardopc1991@masterssh01:~$ cd .ssh/
Leonardopc1991@masterssh01:~/ .ssh$ ls
authorized_keys
Leonardopc1991@masterssh01:~/ .ssh$ nano authorized_keys
Leonardopc1991@masterssh01:~/ .ssh$

```

Ilustración 41: Edición del archivo de llaves autorizadas en el nuevo servidor.

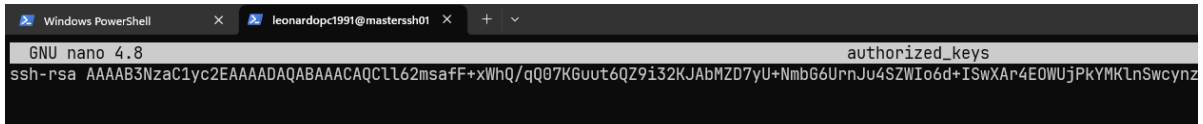


Ilustración 42: Pegaremos el contenido de la llave pública.

En la ilustración 46 podemos ver como se debe configurar al servidor masterssh para que no permita conexiones ssh (secure Shell) de la manera tradicional (usuario y contraseña), para esta tarea usamos el editor de texto nano y modificamos el fichero de configuración sshd\_config el cual se encuentra en el directorio /etc/ssh, dentro del archivo de configuración buscamos PasswordAuthentication, los des comentamos (se le quito el signo del numeral) y como parámetro se configuró no, como se observa en la ilustración 47.

```

Leonardopc1991@masterssh01:~/ .ssh$ sudo nano /etc/ssh/sshd_config
[sudo] password for leonardopc1991:

```

Ilustración 43: Edición del archivo de configuración de SSH.

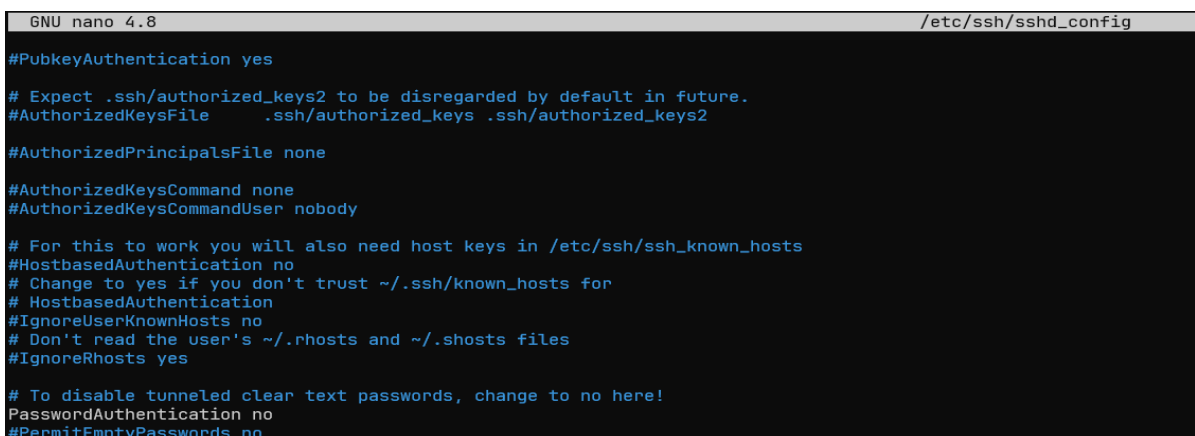


Ilustración 44: Modificaremos la línea tal como se muestra en la imagen.

Para que los cambios surjan efecto se procedió a reiniciar el servicio ssh con

el comando `sudo systemctl restart sshd`. Una característica a nivel de permiso que debe tener la llave es que los permisos deben estar configurados en modo 600 (que el propietario tenga permisos de lectura y escritura) para cambiar los permisos usamos el comando `sudo chmod 600 llave`. Véase la *ilustración 49*.

```
Leonardopc1991@masterssh01:~$ sudo -i chmod 600 llave
```

*Ilustración 45: Cambio de los permisos de la llave.*

Comprobamos que se pueda realizar con éxito los cambios de la llave, para eso utilizamos la cadena de conexión `ssh leonardopc1991@172.31.10.249 -i llave`, con la cual tuvimos una conexión exitosa hacia el servidor remoto que será administrado. Dicha comprobación se puede corroborar en la *ilustración 50*.

```
Leonardopc1991@masterssh01:~$ ls
llave
Leonardopc1991@masterssh01:~$ ssh leonardopc1991@172.31.10.249 -i llave
Enter passphrase for key 'llave':
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-164-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of vie 06 oct 2023 18:50:42 UTC

System load:  0.0          Processes:    244
Usage of /:   10.6% of 58.75GB  Users logged in: 1
Memory usage: 28%          IPv4 address for ens160: 172.31.10.249
Swap usage:  0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

 * Introducing Expanded Security Maintenance for Applications.
Receive updates to over 25,000 software packages with your
Ubuntu Pro subscription. Free for personal use.

https://ubuntu.com/pro

El mantenimiento de seguridad expandido para Applications está desactivado
Se pueden aplicar 50 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Oct 6 18:25:59 2023
Leonardopc1991@keyssh01:~$
```

*Ilustración 46: Ingresaremos al servidor que anteriormente se había configurado la llave SSH id\_rsa*

Una capa adicional que se le otorgó fue la habilitación del firewall, para aquello comprobaremos el estado de `ufw` (Uncomplicated Firewall), para la comprobación se

usó el comando `ufw status` con el cual se comprobó que se encuentra inactivo para ello debe reflejarle como se puede observar en la *ilustración 51*.

```
root@keyssh01:~# ufw status
Status: inactive
root@keyssh01:~#
```

*Ilustración 47: Comprobaremos el estado del firewall de dicho servidor.*

Habilitamos la conexión al puerto 22(ssh/secure Shell) en el servidor remoto, para que solo permita las conexiones desde el servidor centralizado, esto lo logramos con el comando `ufw allow from 172.31.10.242 to any port 22`. Véase la *ilustración 52* para verificar como debe desplegarse el comando.

```
root@keyssh01:~# ufw allow from 172.31.10.242 to any port 22
Rules updated
root@keyssh01:~#
```

*Ilustración 48: Permisos de conexión al puerto 22 solo a la ip indicada que es la ip del servidor master.*

Luego activamos el servicio de firewall con el comando `ufw enable`, por último, para comprobar que se creó la regla ejecutamos el comando `ufw status` y si la regla fue añadida podremos observarla, lo cual se puede evidenciar en la *ilustración 53*

```
root@keyssh01:~# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y/n)? y
Firewall is active and enabled on system startup
root@keyssh01:~# ufw status
Status: active

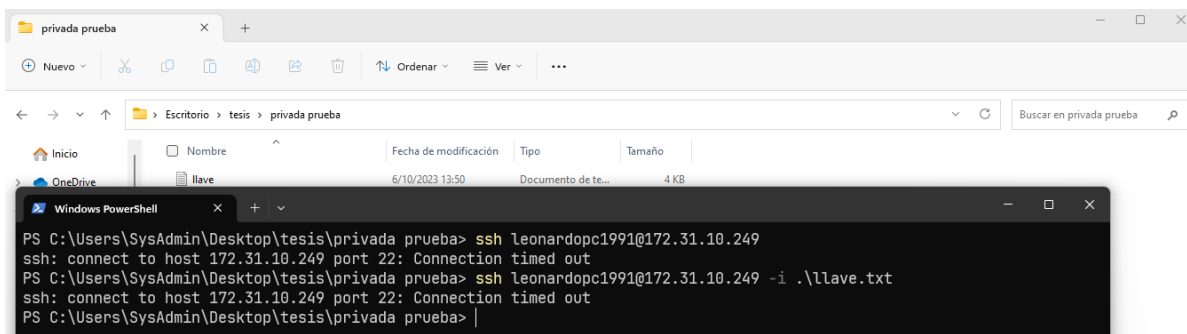
To Action From
--
22 ALLOW 172.31.10.242

root@keyssh01:~#
```

*Ilustración 49: Habilitaremos el firewall y comprobaremos la regla añadida.*

*En la ilustración 55 muestra que, conectarnos al servidor 172.31.10.249 ya*

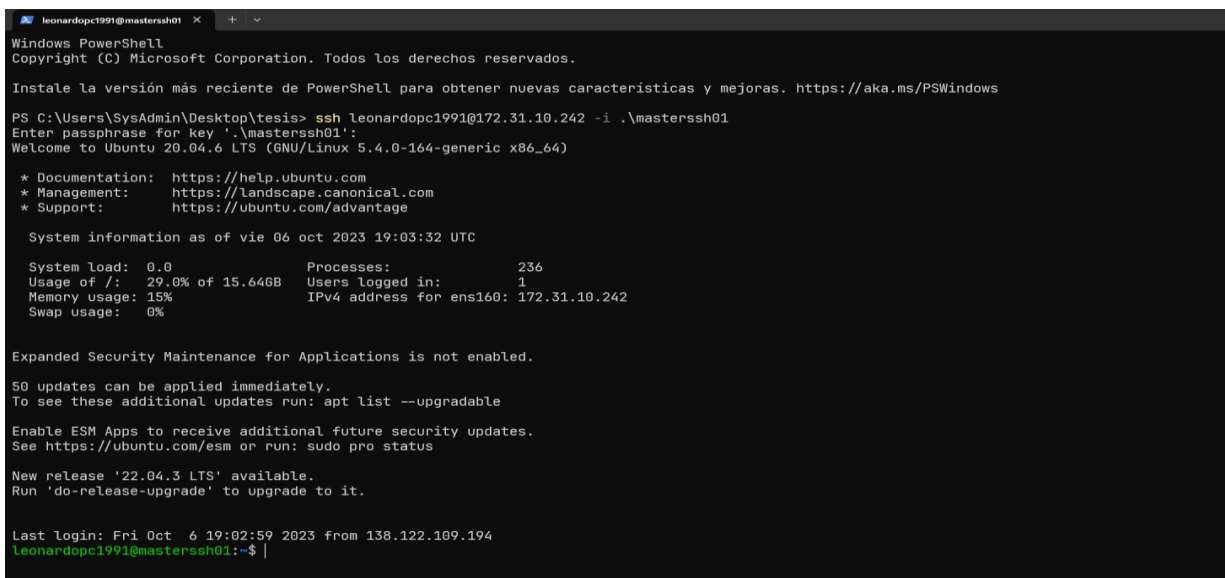
sea pasando por parámetro la llave ssh (secure Shell) o directo, en ambas pruebas nos mostró Connection timed out, lo cual nos indicó que las reglas de firewall fueron configuradas correctamente.



```
PS C:\Users\SysAdmin\Desktop\tesis\privada prueba> ssh leonardopc1991@172.31.10.249
ssh: connect to host 172.31.10.249 port 22: Connection timed out
PS C:\Users\SysAdmin\Desktop\tesis\privada prueba> ssh leonardopc1991@172.31.10.249 -i .\llave.txt
ssh: connect to host 172.31.10.249 port 22: Connection timed out
PS C:\Users\SysAdmin\Desktop\tesis\privada prueba> |
```

*Ilustración 50: Tener en cuenta que, con llave o sin llave no nos permitirá el acceso, ya que solo se dio permiso a la ip del servidor master*

La ilustración 56 se puede observar el inicio de sesión al servidor masterssh haciendo uso de la llave que habíamos configurado en el mismo, y procedimos a conectarnos al servidor 172.31.10.249 el cual solo permite conexiones ssh desde el servidor master 172.31.10.242, en dicha prueba la conexión fue exitosa, al igual como se muestra en la *ilustración 57*.



```
leonardopc1991@masterssh01
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\Users\SysAdmin\Desktop\tesis> ssh leonardopc1991@172.31.10.242 -i .\masterssh01
Enter passphrase for key '.\masterssh01':
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-164-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of vie 06 oct 2023 19:03:32 UTC

System load:  0.0          Processes:    236
Usage of /:   29.0% of 15.64GB  Users logged in:  1
Memory usage: 15%          IPv4 address for ens160: 172.31.10.242
Swap usage:  0%

Expanded Security Maintenance for Applications is not enabled.

50 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Oct 6 19:02:59 2023 from 138.122.109.194
leonardopc1991@masterssh01:~$ |
```

*Ilustración 51: Iniciamos sesión en el servidor master.*

```

Last login: Fri Oct 6 19:02:59 2023 from 138.122.109.194
leonardopc1991@masterssh01:~$ ls
llave
leonardopc1991@masterssh01:~$ ssh leonardopc1991@172.31.10.249 -i llave
Enter passphrase for key 'llave':
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-164-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of vie 06 oct 2023 19:04:02 UTC

System load:  0.0                Processes:    245
Usage of /:   10.6% of 58.75GB    Users logged in: 1
Memory usage: 28%                IPv4 address for ens160: 172.31.10.249
Swap usage:  0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

   https://ubuntu.com/pro

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 50 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Oct 6 19:00:33 2023 from 172.31.10.242
leonardopc1991@keyssh01:~$

```

*Ilustración 52: Comprobación del acceso al servidor.*

## CONCLUSIONES Y TRABAJO FUTURO

La indagación de los distintos mecanismos de encriptación asimétrico facilitó encontrar una estrategia que ayudó a mejorar la seguridad del departamento de servidores de In.Planet S. A. De igual manera esta indagación nos ayudó a identificar cuál de los mecanismos de encriptación asimétrico era el más adecuado para solventar las necesidades existentes en relación con las redes de comunicación utilizadas en el área en la cual se enfocó el proyecto de investigación.

La evaluación de los mecanismos de encriptación asimétrico nos ayudó a identificar cuál de los tres mecanismos resultaba más acorde para dar solución a las necesidades que presenta el departamento de servidores frente ataques criptoanalíticos, fuerza bruta y de otras posibles vulnerabilidades.

Dicha evaluación permitió identificar al mecanismo de encriptación asimétrico RSA como la mejor opción. La selección de RSA resultó ser una opción acertada, pues los resultados en relación a la creación de medidas de seguridad y la correspondiente implementación llevó a la conclusión de que el uso de las llaves públicas y privadas son una alternativa eficiente para proteger la información. Además, las optimizaciones que se realizaron, ayudaron a crear una capa de seguridad aún mayor en conjunto con RSA.

## **RECOMENDACIONES**

Se recomienda realizar nuevos estudios que profundicen la creación de diferentes estrategias que brinde mayores capas de seguridad, ya que el realizar las correspondientes optimizaciones no llevó a la identificación de un nuevo objeto de investigación. De igual forma se recomienda que la implementación de este proyecto se lo aplique en un ambiente no controlado, ya que todo el desarrollo de la propuesta se establecieron parámetros predecibles.



## **BIBLIOGRAFÍA GENERAL:**

- Argüeso Ramirez, E. D. (2019). Propuesta de un sistema de gestión de seguridad de información para la protección de activos de información basado en la norma iso 27001 en el área de informática de la municipalidad provincial De Huánuco.
- Barranco León, M. A. Repositorio de archivos con seguridad basado en el protocolo SSH y el sistema de seguridad RSA.
- Cabanillas Urbina, H. A., & Nizama Ramos, J. J. V. (2022). Análisis de algoritmos de encriptación de datos de texto, una revisión de la literatura científica.
- Cabrera Serrano, X. A. (2023). Análisis comparativo de los modelos de encriptación simétrica y asimétrica (Bachelor's thesis, Babahoyo: UTB-FAFI. 2023).
- Enrique Bonet. (2023). Servicios de acceso remoto II: SSH. Administración y Gestión de Redes S.
- Fernández Orozco, G. (2021). Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientado a la disminución de riesgos en la unidad de informática del GAD municipal del cantón Pujilí.
- Gutiérrez Ruiz, A. D. (2022). Propuesta de modelo de selección de algoritmos criptográficos modernos simétricos y asimétricos incluyendo curvas elípticas aprobadas para entornos informáticos (Doctoral dissertation, Universidad Cenfotec).
- Guerrero, L. S., Abed, M. H., & Quintero, V. G. Análisis de Comparativo de diferentes algoritmos de cifrado (encriptar).
- Hernández (2018). Análisis Comparativo de Cifrado Asimétrico algoritmos RSA y ElGamal. Revista de Sistemas Computacionales y TIC's. Última versión (2018)
- INESDI. (2021). Breve introducción a la Criptografía. Obtenido de INESDI: <https://www.inesdi.com/blog/breve-introduccion-a-la-criptografia/>
- Mayo Vilches, J. (2021). Diseño y simulación firmware de una transmisión de squitters en modo S encriptados mediante RSA.
- Moreno A. & César A. (2018). Estudio de políticas de seguridad para la elaboración de software. <http://hdl.handle.net/10609/81645>
- NQA. (2022). Guía de transición ISO 27001:2022. [www.nqa.com](http://www.nqa.com)
- Serrato Losada, H. D. (2019). Comparación de métodos criptográficos para la seguridad informática.

SSH. (2023). Criptografía. Criptografía explicada.  
<https://www.ssh.com/academy/cryptography>

SSH. (2023). Shell Seguro (SSH). ¿Qué es SSH?  
<https://www.ssh.com/academy/ssh/openssh>

Torres Chango, C. D. (2020). Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada Megaprofer SA (Bachelor's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos).

Yance Sánchez, C. E. (2022). Análisis comparativo de los métodos de encriptación aes y rsa, para las seguridades de los sistemas de información (Bachelor's thesis, Babahoyo: UTB-FAFI. 2022).

Yotam Harchol, Ittai Abraham & Benny Rosas. (2018). Distributed SSH Key Management with Proactive RSA Threshold Signatures. Lecture Notes in Computer Science (LNSC, volumen 10892).

# ANEXOS

## Anexo 1

Entrevista al encargado de servidores:



## Anexo 2

Cuestionario aplicado al encargado de servidores:



