REPOSITORIO DE ARCHIVOS CON SEGURIDAD BASADO EN EL PROTOCOLO SSH Y EL SISTEMA DE SEGURIDAD RSA

Mancer Andrés Barranco León

2080900

Mancerbarranco2890@hotmail.com

REPOSITORIO DE ARCHIVOS CON SEGURIDAD BASADO EN EL PROTOCOLO SSH Y EL SISTEMA DE SEGURIDAD RSA

Mancer Andrés Barranco León

Director de Proyecto

Jaime Vitola Oyaga

Universidad Santo Tomás

Facultad de Ingeniería Electrónica, División de Ingenierías

Bogotá, D.C.

2015

Nota de aceptación:

Firma del Director de Proyecto

Firma del Jurado

Firma del Jurado

Contenido

Lista de figuras

Pág.

Lista de tablas

Pág.

Lista de Anexos

Pág.

Resumen

Este proyecto posee elementos de investigación, diseño e implementación, basados en el conocimiento adquirido durante el transcurso de la carrera de Ingeniería Electrónica. Dichos elementos se han aplicado en la implementación de un repositorio con seguridad basado en el protocolo SSH y el sistema de seguridad RSA.

El diseño de este repositorio con seguridad está conformado por una serie de máquinas virtuales implementadas en el software libre virtualizador VirtualBox, que representan los diferentes departamentos de la empresa Orange Business Services (Operaciones, Ventas y Finanzas) con diferentes sistemas operativos (Windows XP y Linux). Además se cuenta con la implementación de un servidor de llaves públicas (Ubuntu Server Keys) las cuales serán utilizadas para el proceso de encriptación y des-encriptación de archivos.

La aplicación directa de este proyecto se verá reflejada en el ejercicio de encriptación, almacenamiento, des-encriptación y descarga de archivos, con la interacción de los diferentes usuarios de los departamentos de la empresa.

Introducción

Orange Business Services Colombia S.A, es una empresa multinacional dedicada a la integración de soluciones en telecomunicaciones para empresas multinacionales tales como la comercialización de servicios como routing, switching, hosting, administración y automatización de redes, seguridad, wireless y comunicaciones unificadas, a su vez comercializa equipos de marcas como Cisco, Riverbed, Polycom, entre otras.

Teniendo en cuenta lo anterior, Orange es una empresa que está en constante innovación en cuanto a sus aplicativos y herramientas para organizar de manera eficiente los procesos internos y así brindar un mejor servicio al cliente. Es aquí donde se presenta un crecimiento de los contenidos digitales, donde la empresa se ve obligada a asegurar la preservación de la información mediante el uso de aplicaciones que permitan garantizar la autenticidad, integridad, seguridad, privacidad y protección de datos generando una mejor organización de la información de la empresa.

Este proyecto se diseñó e implementó con la finalidad de plantear una solución al problema de la seguridad de archivos entre los departamentos de la empresa Orange Business Services, ya que actualmente se trabajan con repositorios de información que sólo organizan los archivos pero no tienen seguridad ni privacidad entre departamentos.

En el ámbito social la seguridad de la información es un campo de vital importancia debido a los diferentes cambios que se presentan a nivel mundial actualmente hablando del crecimiento de contenidos digitales. Por tal motivo desde el punto de vista de la ingeniería electrónica, se brinda un servicio de seguridad a bajo costo que ofrece la privacidad y seguridad requerida para la empresa.

Desde el ámbito de la comprensión humanística brindada por el enfoque humanista-cristiano de la Universidad Santo Tomás, se propone una solución que aporte a la construcción de la realización del bien común a nivel nacional e internacional mostrando a través de las herramientas utilizadas a lo largo del proyecto, una manera para reducir la exclusión social, económica, cultural y política; permitiendo una formación integral desde una perspectiva personal y profesional, con el fin de aportar a la evolución, innovación y progreso para el sector laboral.

Capítulo I

Introducción e información preliminar

1. Descripción del Problema

En la actualidad se evidencian cambios tecnológicos de manera acelerada que facilitan en dispositivos y herramientas el manejo de aplicativos más avanzados y tecnificados; lo que permite brindar calidad en el desarrollo e innovación de nuevos servicios en el campo del almacenamiento seguro en la red. En este ámbito se presenta un crecimiento de los contenidos digitales en las organizaciones de manera que surge la obligación de asegurar la preservación de la documentación mediante el uso de aplicaciones que permitan garantizar la autenticidad, integridad, seguridad, privacidad y protección de datos que proporcionen escalabilidad y facilidad de manejo a los usuarios; generando una mejor calidad de trabajo, eficiencia de los procesos internos y mejor organización de la información de la empresa .

Teniendo en cuenta esto, se pretende brindar a la empresa un servicio repositorio de archivos con seguridad implementado en Ubuntu Server con un sistema de liberación de claves y encriptación asimétrica implementada en el protocolo SSH (Secure SHell), basado en el sistema de seguridad RSA. Este servicio lo conforman máquinas virtuales que representan ordenadores físicos de diferentes departamentos o sectores de la empresa que depositan información y datos confidenciales de alta importancia (archivos con bases de datos, Excel, Word, entre otros), en una máquina virtual en común (repositorio digital) de manera que al consultar sus datos, el sistema pida contraseñas o claves propias de cada departamento con la ayuda de la encriptación asimétrica por el protocolo SSH, para brindar mayor seguridad al proceso.

2. Antecedentes

Antes de dar a conocer los repositorios digitales y sus antecedentes, es necesario dar a conocer un tema que va ligado a estos y es la preservación digital. Se define como el conjunto de métodos que garantizan que la información digital almacenada sin importar el formato, programa u ordenador físico en el que se haya creado, pueda mantenerse y seguir utilizándose en el futuro teniendo en cuenta los cambios tecnológicos y otros factores que puedan afectar la información.
Sin embargo la preservación digital no sólo es una tarea exclusiva de las bibliotecas y universidades ya que vincula a todos los actores relacionados con la creación, gestión y uso de cada documento digital.

Teniendo en cuenta lo anterior se han realizado investigaciones acerca de la preservación digital por parte de bibliotecas, universidades, empresas de software, archivos nacionales e instituciones depositarias de documentación en países europeos, Oceanía y Estados Unidos, para ofrecer aplicaciones de preservación de la información como repositorios digitales en diferentes entornos como lo son institucionales, archivos administrativos, archivos personales, entre otros.

Algunos de los repositorios de archivos digitales enfocados principalmente en el ámbito académico a nivel internacional se conocen los siguientes:

- Social Science Research Network (SSRN):
  Es un repositorio online para consultas académicas donde permite compartir de forma rápida y eficaz trabajos entre autores y lectores, el objetivo principal de esta es incentivar la investigación en ciencias sociales. (Página WEB: **http://www.ssrn.com/en/**)

- SEDICI:
  Es un repositorio institucional de la Universidad Nacional de la Plata, creado para preservar, difundir y guardar todas las producciones intelectuales, científicas y artísticas de la comunidad universitaria (estudiantes, profesores e investigadores). Es de acceso abierto lo cual toda su información se puede encontrar de forma gratuita. (Página WEB: **http://sedici.unlp.edu.ar/**)

- Digital.C SIC:
  Repositorio científico multidisciplinar que recoge los diferentes resultados de las investigaciones realizadas en los centros e institutos del CSIC (Centro Superior de Investigaciones Científicas) con acceso abierto. (Página WEB: **http://digital.csic.es/?locale=es**)

- Repositorio DSpace@Cambridge:
  Este repositorio de la Universidad de Cambridge ofrece el servicio gestionado por la biblioteca y el servicio de informática, donde pretende difundir y preservar los materiales digitales creados por las personas vinculadas y no vinculadas de la universidad. En este se proporcionan artículos, informes técnicos, tesis, entre otros. (Página WEB: **https://www.repository.cam.ac.uk/**)

- Acceda:
  Es un repositorio digital de la Universidad de Las Palmas de Gran Canaria (ULPGC) en España, el cual fue creado para la recolección de información científica de los estudiantes, docentes, investigadores y personal administrativo.
  El repositorio cuenta con la aplicación BUStreaming, el cual convierte videos y audio FLASH en Streaming con un sistema de auto publicación. (Página WEB**:** **http://acceda.ulpgc.es/**)

- Recolecta:
  Esta plataforma conocida también como Recolector de ciencia abierta, es un repositorio que agrupa todos los repositorios científicos de España y provee se servicios a los gestores de los repositorios, a los investigadores y al personal encargado de la elaboración (Página Web: **http://recolecta.fecyt.es/**)

- Red de repositorios Latinoamericanos:
  Es una plataforma que tiene como objetivo el ofrecer una herramienta de fácil acceso a las publicaciones digitales en texto completo de diferentes repositorios en Latinoamérica como Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guyana, Honduras, México, Perú, Puerto Rico, Trinidad y Tobago y Uruguay. (Página WEB: **http://www.repositorioslatinoamericanos.info/**)

Actualmente los repositorios disponibles a nivel nacional más reconocidos en el ámbito académico son:

- Repositorio UNAL:
  Encargado de brindar información académica y científica como tesis de grado, posgrado e investigaciones originales. La información se encuentra de forma gratuita. (Página WEB: **http://www.bdigital.unal.edu.co/**)

- Biblioteca digital Universidad del Valle:
  Es un repositorio con el fin de preservar y divulgar la producción intelectual de los miembros de la comunidad universitaria y las obras de diferentes autores e instituciones pertenecientes a proyectos de alcance regional. (Página WEB: **http://bibliotecadigital.univalle.edu.co/**)

- Biblioteca digital Universidad de Antioquia:
  Plataforma en la que se puede publicar, consultar y descargar documentos en texto de la producción científica, académica, cultural y patrimonial de la comunidad universitaria (Página WEB: **http://tesis.udea.edu.co/dspace/**)

- Repositorio Académico de la Universidad Tecnológica de Pereira:
  Repositorio de acceso libre para consultar documentos académicos, producción académica y editorial, seminarios de grado, tesis y disertaciones, trabajos de grado; de la comunidad universitaria. (Página WEB: **http://repositorio.utp.edu.co/dspace/**)

- Biblioteca Digital Pontificia Universidad Javeriana:
  Plataforma de acceso libre donde pueden ser consultados, descargados, impresos y distribuidos públicamente archivos académicos que no sean de título comercial ni con fines de lucro.
  Se pueden consultar archivos relacionados con las facultades de Ciencias sociales, Educación, Artes, Psicología, Medicina, Odontología, Ingeniería, entre otras. (Página WEB: **http://repository.javeriana.edu.co/**)

Por otro lado, existen repositorios digitales con seguridad enfocados al almacenamiento y generación de certificados digitales, entre los cuales se encuentra:

- ICB BRASIL:
  Es una plataforma con infraestructura de clave Pública de Brasil que permite la emisión de certificados digitales para la identificación virtual del ciudadano, regido por las normas del Instituto Nacional de Tecnologías de la Información (ITI).
  El ICB BRASIL tiene diferentes funciones como AC Root (El certificado de autoridad raíz que permite la gestión y distribución de certificados), AC (Autoridad de Certificación, se encarga de verifica que el titular del certificado tenga la clave privada correspondiente al clave pública que forma parte del certificado, firma digital del certificado del suscriptor para garantizar la identidad del titular), AR (Autoridad de Registro, es la interfaz entre el usuario y la autoridad de certificación la cual tiene como objetivo la recepción, validación y renovación de certificados digitales), entre otras.

En términos generales la ICB Brasil asegura que los visitantes, usuarios y clientes mantengan un intercambio seguro de información sin que esta sea interceptada o alterada, gracias al protocolo de encriptación SSL (Secure Sockets Layer) que permite los siguientes beneficios:

- Garantizar la seguridad de los sitios protegidos en las búsquedas en Google.
- Utilizar el sello de sitio seguro o seguridad en la web brasileña.
- Utilización de servicios gratuitos como evaluación de vulnerabilidad, diario de análisis de malware y sellar en la búsqueda.

(Página WEB: **http://icp-brasil.certisign.com.br/repositorio/index.htm**)

3. Justificación

La implementación de un repositorio con seguridad, que por medio del protocolo SSH y el sistema de seguridad RSA de encriptación asimétrica pueda dar acceso a los archivos correspondientes a cada departamento mediante la generación de claves o contraseñas propias de cada uno garantizando la organización, confidencialidad, integridad, disponibilidad, utilidad y privacidad de los datos e información que se maneja en la empresa para generar eficiencia en los procesos internos de cada departamento, mejorar la calidad de trabajo y la organización de la información.

4. Objetivo General

Implementar un servicio repositorio con seguridad de fácil manejo que garantice el orden, control, privacidad y seguridad de la información de la empresa.

4.1. Objetivos Específicos

1. Proporcionar un sistema de fácil manejo para la empresa.

2. Utilizar herramientas de software libre que generen bajo costo de implementación a la empresa.

3. Ofrecer un servicio repositorio con seguridad que garantice la confianza y seguridad de la información de la empresa y a su vez genere eficiencia en los procesos internos de cada departamento.

4. Mantener el óptimo desarrollo del sistema de liberación de claves mediante el protocolo SSH de encriptación asimétrica y el sistema de seguridad RSA.

5. Garantizar el funcionamiento de la comunicación entre las máquinas virtuales y el repositorio con seguridad.

6. Identificar las ventajas que proporciona la implementación del servicio repositorio con seguridad en la empresa.

5. Factibilidad

El sistema repositorio con seguridad es un servicio innovador ya que actualmente no es muy competido en el mercado y brinda a la empresa seguridad, orden, control y fácil manejo de los archivos, ya que mediante la implementación del software virtualizador VIRTUAL BOX permite visualizar el comportamiento de los ordenadores asignados a los diferentes departamentos de la empresa comunicándose con el repositorio con el apoyo del proceso de encriptación asimétrica SSH y el sistema de seguridad RSA.
Teniendo en cuenta lo anterior, se ofrece un servicio a bajo costo que garantiza seguridad y facilidad de adaptación al medio en él que se encuentre; además de generar eficiencia en los procesos internos de la empresa, gracias a las características principales que debe cumplir la preservación digital como lo es la confidencialidad, integridad, disponibilidad, utilidad, organización y fácil manejo de la información.

Capítulo II

Marco Teórico

Al implementarse el servicio repositorio, es importante aclarar conceptos relacionados con la seguridad y encriptación de archivos, comunicación entre ordenadores y demás temas que permitan una fácil comprensión del proceso a realizar.

6. Repositorio Digital

Primero que todo, repositorio digital es un sitio centralizado en el que se almacena y mantiene información digital (bases de datos, imágenes, entre otros), los cuales se usan en la mayoría de casos en ambientes académicos como universidades, centros de investigación, etc. Sin embargo también son aplicables a cualquier ámbito en el que se necesite compartir y almacenar información de interés. Los datos almacenados en un repositorio pueden distribuirse a través de internet o un medio físico como un disco compacto, de manera que pueden ser de acceso público o tener restricciones de privacidad los cuales necesitan una autenticación previa.

Actualmente los repositorios suelen tener sistemas de respaldo y mantenimiento correctivo para la preservación de la información en caso de que la máquina física quede inutilizable, a este procedimiento se le conoce como preservación digital.

La elección del software es una cuestión crucial para la implementación de un repositorio digital, para ello debe cumplir los siguientes requerimientos:

- Apoyo a los diferentes formatos de archivo, escalabilidad, extensibilidad y mantenimiento del sistema.
- Inter-operatividad (que pueda cumplir con los principales protocolos de intercambio de registros de información).
- Localización permanente de los documentos, mediante incorporación de identificadores persistentes de objetos digitales (DOI – Identificación de material digital).
- Aplicaciones de búsqueda y visualización de metadatos.
- Interfaz de búsqueda a texto completo.
- Personalización de software

Algunas instituciones promueven el uso de sus repositorios como un servicio adicional para el investigador. Otras instituciones poseen mandatos propios que obligan a los autores o investigadores a depositar sus publicaciones (o determinados tipos, como por ej. tesis doctorales) en el repositorio institucional, con fines de visibilidad, impacto y preservación. En algunos países, como por ejemplo Argentina, se han promulgado leyes de acceso abierto que promueven la implementación y uso de los repositorios de instituciones sustentadas con fondos públicos, mientras que otros países están trabajando en la aprobación de leyes similares, como por ejemplo México.

Teniendo en cuenta lo anterior, se puede empezar a abordar el tema de la seguridad de archivos, y lo primero que se debe mencionar es la encriptación que está definida como un método con el que

se protegen archivos, documentos y datos, el cuál funciona a través de la utilización de códigos o cifras para escribir un mensaje de forma secreta. El proceso por el cual se cifra un mensaje, se denomina criptografía la cuál es la creación de técnicas para el cifrado de datos e información.

7. Criptografía

La criptografía se divide a su vez en dos clases diferentes:

7.1. Criptografía simétrica

Este tipo de criptografía es conocida como criptografía de clave secreta o de una sola clave ya que solo se usa una misma clave para cifrar y descifrar los mensajes. Esto quiere decir que se tiene acceso al mensaje cuando el remitente del mensaje realiza el proceso de cifrado mediante una clave y el receptor descifra el mensaje con la misma clave.
La desventaja de este sistema es que actualmente los ordenadores pueden descifrar claves con bastante facilidad, de manera que un atacante podrá consultar las claves usadas entre emisor y receptor por el canal de comunicación que se utilice y descifrar el mensaje.

7.2. Criptografía asimétrica

Sistema conocido como criptografía de clave pública o criptografía de dos claves, donde el emisor del mensaje tiene una clave pública (clave que se entrega a cualquier persona) y una clave privada (Esta clave la debe tener únicamente el propietario).
El proceso de cifrado consiste en que el emisor cifra el mensaje con la clave pública del receptor y es el receptor descifra el mensaje con la clave privada. De lo anterior podemos decir que es un sistema seguro ya que no se necesita el envío de claves.
La desventaja del proceso de encriptación asimétrica se puede visualizar en la siguiente imagen:

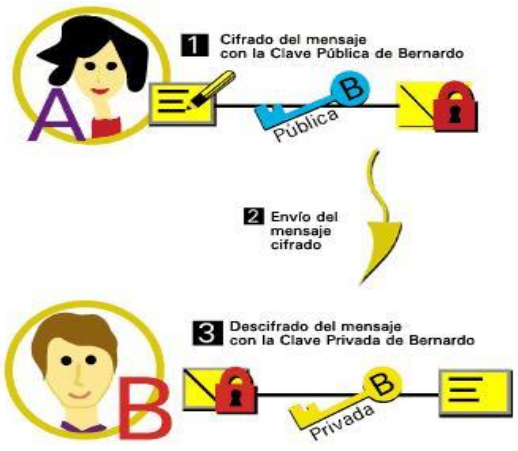


Fig.1. Proceso de encriptación asimétrica - Imagen tomada de:
http://katherynnparedes.blogspot.com.br/2013/04/tipos-de-protocolo.html

Teniendo en cuenta los conceptos anteriores se puede llegar a entender de mejor forma el protocolo de encriptación asimétrica SSH que se utilizara para la implementación del servicio.

8. Protocolo SSH

El protocolo SSH o más conocido como "Secure Shell" (Interprete de órdenes seguro) nombre que también identifica al programa, es utilizado para acceder a máquinas virtuales remotas a través de una red. SSH usa técnicas de cifrado que hacen que la información viaje por el medio de manera legible, garantizando que ninguna tercera persona pueda descubrir el usuario, la contraseña de conexión ni lo que se escribe durante toda la sesión.

Por otra parte SSH usa criptografía de llave pública para autenticar el equipo remoto y permitir al mismo autenticar al usuario si es necesario, sin embargo también permite el reenvío de puertos TCP de forma arbitraria y de conexiones X11 (Tecnología que permite ejecutar sesiones X11 remotas de manera rápida y con excelente calidad gráfica, fue desarrollada por la compañía francesa NoMachine, la cual ofrece aplicaciones cliente y servidor de manera gratuita (pero no libre) y también de manera comercial). Un servidor SSH por defecto, escucha el puerto TCP 22. Un programa cliente de SSH es utilizado generalmente para establecer conexiones a un dominio sshd que acepta conexiones remotas. Ambos se encuentran comúnmente en los sistemas operativos más modernos, incluyendo Mac OS X, Linux, Solaris y OpenVMS.

Existen actualmente dos versiones de SSH (versión 1 y versión 2).

Versión 1 (SSHV1):

La versión 1 de SSH hace uso de muchos algoritmos de encriptación patentados (algunas de estas patentes han expirado) sin embargo son vulnerables en cuanto a seguridad ya que potencialmente permiten a un intruso insertar datos en la corriente de comunicación.

Versión 2 (SSHV2):

El paquete OpenSSH bajo Red Hat Enterprise Linux utiliza la versión 2 de SSH por defecto, pues esta versión del protocolo tiene un algoritmo de intercambio de llaves que no es vulnerable en cuanto a seguridad. Sin embargo, la suite OpenSSH también soporta las conexiones de la versión 1.
Para el caso del proyecto se manejará la versión 2 del protocolo SSH utilizado tanto en el paquete Open SSH (Linux) y Putty (Windows).

Hablando un poco de la transferencia de datos, SSH permite realizar el intercambio de información usando protocolos tales como SFTP (Conocido como el protocolo seguro de transferencia de archivos, permite capacidades de transferencia segura de archivos entre ordenadores conectados en red) o SCP (Conocido como copia segura o SCP es un medio para transferir de forma segura archivos entre un host local y un control remoto de host o entre dos hosts remotos. Se basa en el protocolo (SSH)) asociados.
También permite gestionar claves RSA para no escribir claves al establecer conexión a algún dispositivo y transferir los datos de cualquier otra aplicación por un canal seguro tunelizado

(Referente a aquellos protocolos tunelizados donde dividen el mensaje en diferentes partes (normalmente 2): una que contiene los datos reales que se están transmitiendo y otra que contiene la información sobre las reglas de la transmisión. Con el fin de que se establezca la conexión, ambas partes deben comprender y utilizar el mismo protocolo de comunicaciones. Esencialmente, crea un túnel entre dos puntos de una red por el cual se puede transmitir de forma segura cualquier tipo de dato).

Algunas características destacadas del protocolo SSH son:

- El usuario transmite la información al servidor usando encriptación robusta (llaves de 128bits).
- El uso de encriptación de 128 bits en recepción y transmisión de la información, garantiza la seguridad y hace complejo el descifrado.
- Ayuda a proporcionar seguridad a protocolos inseguros por medio de la técnica de reenvío por puerto.
- En cuanto a confidencialidad, el protocolo SSH a diferencia de protocolos como el TSL (Transport Layer Security) aplica un cifrado simétrico a los datos de manera que será necesario realizar previamente un intercambio seguro de claves entre cliente y servidor.
  En la versión 2 de SSH se pueden utilizar algoritmos de cifrado distintos en los dos sentidos de la comunicación.
  Un servicio adicional que proporciona SSH es la confidencialidad de la identidad del usuario. Mientras que en SSL 3.0 y TLS 1.0, si se opta por autenticar al cliente, éste tiene que enviar su certificado en claro (sin emcriptar), en SSH (y también en SSL 2.0) la autenticación del usuario se realiza cuando los paquetes ya se mandan cifrados.
- En cuanto a la autenticidad, SSH proporciona mecanismos para autenticar tanto el ordenador servidor como el usuario que se quiere conectar.
  La autenticación del servidor suele realizarse conjuntamente con el intercambio de claves. En SSH2 el método de intercambio de claves se negocia entre el cliente y el servidor, aunque actualmente sólo hay uno definido, basado en el algoritmo de Diffie-Hellman.
  Para autenticar al usuario existen distintos métodos; dependiendo de cuál se utilice, puede ser necesaria también la autenticación del ordenador-cliente, mientras que otros métodos permiten que el usuario debidamente autenticado acceda al servidor desde cualquier ordenador cliente.
- En eficiencia, SSH utiliza la compresión de los datos transferidos para reducir la longitud de los paquetes. SSHen su versión 2 permite negociar el algoritmo que se utilizará en cada sentido de la comunicación, aunque solamente existe uno.
  A diferencia de SSL/TLS, en SSH no está prevista la reutilización de claves de sesiones anteriores: en cada nueva conexión se vuelven a generar nuevas claves.
  Para el caso de SSH se tiene pensado para conexiones que tienen una duración más o menos larga, como suelen ser las sesiones de trabajo interactivas con un ordenador remoto y no para las conexiones cortas pero consecutivas las cuales son más comunes del protocolo de aplicación HTTP (que es el que inicialmente se quería proteger con SSL).

Para realizar una conexión entre dos equipos (servidor-cliente) mediante el protocolo SSH se deben seguir la siguiente secuencia de eventos:

- Primero se lleva a cabo un 'handshake' (apretón de manos - establece de forma dinámica los parámetros de un canal de comunicaciones entre dos equipos antes de que comience la

comunicación normal por el canal) encriptado para que el cliente pueda verificar que se está comunicando con el servidor correcto.

- La capa de transporte de la conexión entre el cliente y la máquina remota es encriptada mediante un código simétrico.

- El cliente se autentica ante el servidor.

- Por último el cliente remoto interactúa con la máquina remota sobre la conexión encriptada.

Cabe dar explicación a una parte importante como lo es la capa de transporte la cual tiene el papel de facilitar una comunicación segura entre los dos equipos (servidor-cliente) durante la autenticación y la comunicación. La capa de transporte lleva esto a cabo manejando la encriptación y decodificación de datos, proporcionando protección de integridad de los paquetes de datos mientras son enviados y recibidos. Además, la capa de transporte proporciona compresión de datos, lo que acelera la transmisión de la información.
Al contactar un cliente a un servidor por medio del protocolo SSH, se negocian varios puntos importantes para que ambos sistemas puedan construir la capa de transporte correctamente.
Durante el intercambio se producen los siguientes pasos:

- Intercambio de claves
- Se determina el algoritmo de encriptación de la clave pública
- Se determina el algoritmo de la encriptación simétrica
- Se determina el algoritmo autenticación de mensajes
- Se determina el algoritmo de hash que hay que usar

El servidor se identifica ante el cliente con una llave de host única durante el intercambio de llaves. Obviamente si este cliente nunca se había comunicado antes con este determinado servidor, la llave del servidor le resultará desconocida al cliente y no lo conectará.
OpenSSH evita este problema permitiendo que el cliente acepte la llave del host del servidor después que el usuario es notificado y verifica la aceptación de la nueva llave del host. Para las conexiones posteriores, la llave del host del servidor se puede verificar con la versión guardada en el cliente, proporcionando la confianza de que el cliente se está realmente comunicando con el servidor deseado.
Si en un futuro la llave del host ya no coincide, el usuario debe eliminar la versión guardada antes de que una conexión pueda ocurrir.
SSH fue diseñado para funcionar con casi cualquier tipo de algoritmo de clave pública o formato de codificación. Después del intercambio de claves inicial se crea un valor hash usado para el intercambio y un valor compartido secreto, los dos sistemas empiezan inmediatamente a calcular claves y algoritmos nuevos para proteger la autenticación y los datos que se enviarán a través de la conexión en el futuro.
Después que una cierta cantidad de datos haya sido transmitida con un determinado algoritmo y clave (la cantidad exacta depende de la implementación de SSH), ocurre otro intercambio de claves, el cual genera otro conjunto de valores de hash y un nuevo valor secreto compartido. De esta manera aunque un agresor lograse determinar los valores de hash y de secreto compartido, esta información sólo será válida por un período de tiempo limitado.

Para dar mejor claridad al proceso explicado anteriormente, se tiene en cuenta la siguiente imagen:

Fig.2. Funcionamiento del protocolo SSH (Identificación SSH mediante clave)- Imagen tomada de: http://katherynnparedes.blogspot.com.br/2013/04/tipos-de-protocolo.html

Dando continuidad con el proceso explicado anteriormente, es necesario dar a conocer el proceso de autenticación cuando en la capa de transporte se haya construido el medio seguro para transmitir información entre los dos sistemas, el servidor le dirá al cliente de los diferentes métodos de autenticación soportados, tales como el uso de firmas privadas codificadas con claves o la inserción de una contraseña. El cliente entonces intentará autenticarse ante el servidor mediante el uso de cualquiera de los métodos soportados.
Los servidores y clientes SSH se pueden configurar para que permitan varios tipos de autenticación, lo cual le concede a cada lado la cantidad óptima de control. Luego el servidor podrá decidir qué métodos de encriptación soportará basado en su pauta de seguridad, y el cliente puede elegir el orden en que intentará utilizar los métodos de autenticación entre las opciones a disposición. Gracias a la naturaleza segura de la capa de transporte de SSH, hasta métodos de autenticación que parecen inseguros, como la autenticación basada en contraseñas, son en realidad seguros para usar.

Para el caso del proyecto se debe tener presente la configuración del paquete OpenSSH en el sistema operativo Linux, donde se implementará el repositorio con seguridad.
OpenSSH (OpenBSD Secure Shell) es un conjunto de programas de computadora que proveen una sesión de comunicación encriptada en una red informática que utiliza el protocolo SSH. Fue creado como una alternativa de código abierto al software propietario ofrecido por SSH Communications Security. OpenSSH es desarrollado como parte del proyecto OpenBSD, que está a cargo de Theo de Raadt.
Este programa es confundido a veces con OpenSSL por la similitud de nombre, sin embargo, los proyectos tienen objetivos distintos y están desarrollados por equipos diferentes.
Para la instalación del paquete es necesario poner el siguiente comando en la consola del cliente:

Instale openssh

Una vez instalado el paquete en el repositorio se procede a configurar el programa mediante el siguiente comando:

/etc/ssh/sshd_config

Actualmente ya no es necesario especificar la versión del protocolo a implementar ya que por defecto el programa está configurado con la versión 2 de SSH.
A continuación se deben agregar las siguientes líneas de comando para completar la configuración del programa:

- Para brindarle acceso sólo a algunos usuarios:

AllowUsers user1 user2 userX

- Para permitir el acceso sólo a algunos grupos:

AllowGroups group1 group2 group X

- Para deshabilitar el acceso a root por SSH se debe cambiar la línea PermitRootLogin:

PermitRootLogin no

Como bien se puede apreciar es una configuración básica para poner en funcionamiento el programa, sin embargo se tiene algunas recomendaciones tales como:

- Es posible que el usuario desee cambiar el puerto por defecto de 22 a cualquier puerto superior. A pesar de que el puerto SH que está siendo ejecutado puede ser detectado utilizando un port-scanner o escáner de puertos como NMAP, cambiarlo reducirá el número de entradas en el log causados por intentos de autentificación automáticos. Para ayudar a seleccionar un puerto, se debe revisar la lista de números de puerto TCP y UDP. Para verificar la distribución de los puertos a nivel local se introduce en la consola el comando */etc/services*. Se selecciona un puerto alternativo que no esté ya asignado a un servicio común para evitar conflictos.
- Se deben desactivar los inicios de sesión con la contraseña ya que esto aumenta el grado de seguridad del sistema.

Ahora en el caso del repositorio con seguridad (servidor) se deben agregar los siguientes comandos para su configuración:

 # Package generated configuration file
 # See the sshd_config(5) manpage for details

Se asigna el puerto por el cual el protocolo SSH se va a comunicar, por defecto es el 22. Se debe abrir un puerto en el equipo redirigiendo hacia la IP interna de la máquina donde se tenga.

Port 1234

Ahora se asigna la versión del protocolo SSH a usar, para este caso se utiliza el protocolo 2 (versión 2 de SSH ya que es más seguro y confiable.

Protocol 2

Si se está utilizando el protocolo SFTP (SSH File Transfer Protocol) teniendo los clientes o grupos enjaulados, se deben poner los siguientes comandos teniendo en cuenta que la línea *Subsystem sftp /usr/lib/openssh/sftp-server* debe ir en comentario.

Subsystem sftp internal-sftp
Match user server
ChrootDirectory /home/jail/home
AllowTcpForwarding no
ForceCommand internal-sftp

9. Sistema de Seguridad RSA

Es un sistema de seguridad el cual utiliza el método de criptografía de llave pública utilizada para el cifrado de información y firma digital (son aquellas que no tienen alteraciones en archivos digitales). RSA es un sistema con alta seguridad ya que utiliza dos problemas matemáticos: La factorización de números grandes (usando el método teniendo 663 bits de longitud usando técnicas de distribución avanzada) y El descifrado RSA (es un problema que actualmente los computadores no pueden resolver por falta de un algoritmo eficiente).

Hablando acerca de la historia del sistema RSA, fue creado en 1978 por Rivest, Shamir y Adlman con la idea de implementar un sistema criptográfico asimétrico que actualmente es el más conocido y usado. Estos señores se basaron en el artículo de Diffie-Hellman sobre sistemas de llave pública, crearon su algoritmo y fundaron la empresa RSA Data Security Inc., que es actualmente una de las más prestigiosas en el entorno de la protección de datos.

Hablando un poco acerca de los métodos que existen para encriptar o des-encriptar información, existe la criptografía de clave secreta la cual consiste en que tanto emisor como receptor conocen y utilizan la misma clave secreta para cifrar y descifrar mensajes.
Sin embargo se deben tener presentes algunas desventajas tales como:

- El emisor y el receptor deben ponerse de acuerdo con la clave secreta a manejar.
- Se debe poner en común el medio fiable para la transferencia de archivos.
- Cualquier persona externa al proceso puede interceptar la clave y podrá ver la información encriptada.
- Presenta dificultad para proporcionar una administración segura de las claves.

Por lo anterior se hace más confiable la utilización del sistema RSA.

El sistema RSA se basa en el hecho matemático de la dificultad de factorizar números muy grandes. Para factorizar un número el sistema más lógico consiste en empezar a dividir sucesivamente éste entre 2, entre 3, entre 4 y así sucesivamente buscando que el resultado de la división sea exacto, es decir, de resto 0 con lo que ya tendremos un divisor del número.

Si el número considerado es un número primo (el que sólo es divisible por 1 y por él mismo), se tiene que para factorizarlo habría que empezar por 1, 2, 3, y así sucesivamente hasta llegar a él mismo, ya que por ser primo ninguno de los números anteriores es divisor suyo.
Ahora si el número primo es lo suficientemente grande, el proceso de factorización es complicado y lleva mucho tiempo.

Teniendo presente lo anterior el sistema RSA crea sus claves de la siguiente manera:

- Primero se deben buscar dos números primos lo suficientemente grandes (p y q - entre 100 y 300 dígitos).
- Se obtienen los números bajo las siguientes operaciones (n = p * q) y (Ø = (p-1) * (q-1)).
- Se halla un número tal que no tenga múltiplos comunes con la operación Ø.
- A continuación se calcula la exponente del módulo (d = e-1 mod Ø), con mod = resto de la división de números enteros.
- Una vez se hayan obtenido estos números, el valor "n" es la clave pública y "d" es la clave privada. Los números p, q y Ø se destruyen. También se hace público el número e, necesario para alimentar el algoritmo.

El proceso de encriptación y des-encriptación se lleva a cabo gracias a los siguientes pasos:

- Primero se deben encontrar dos números primos largos "p" y "q" de forma aleatoria y definir el valor de "n" (valor del módulo) con la operación: n= p*q.
- Ahora se debe encontrar un número entero largo "d" que sea relativamente primo a la operación (p-1 (q-1).
- Luego se escoge un número primo que pertenezca al intervalo (max(p,q)+1, n-1), donde se tendrá la pareja [d, (p-1)(q-1)]=1.
- A continuación se debe obtener un número entero "e" que este dentro del rango 1< e < (p-1) (q-1) realizando la operación (e*d =1 mod(p-1)(q-1)).
- Se obtiene la clave pública formada por la pareja (n,e) y la clave privada por la pareja (n,d).
- Partiendo de las claves generadas anteriormente, se asocia a cada carácter del alfabeto un valor numérico en el rango de (1,…n) donde se procede a cifrar el mensaje "m" por bloques de la misma longitud.
- Para cifrar cada uno de los mensajes "m", se realiza la siguiente operación C=M^(e) * mod (n)
- Para descifrar C y obtener la información real del mensaje "m" se utiliza la clave privada "d" mediante la operación m= C^(d) *mod(n).

El proceso anterior se visualiza de mejor manera gracias a la siguiente imagen:

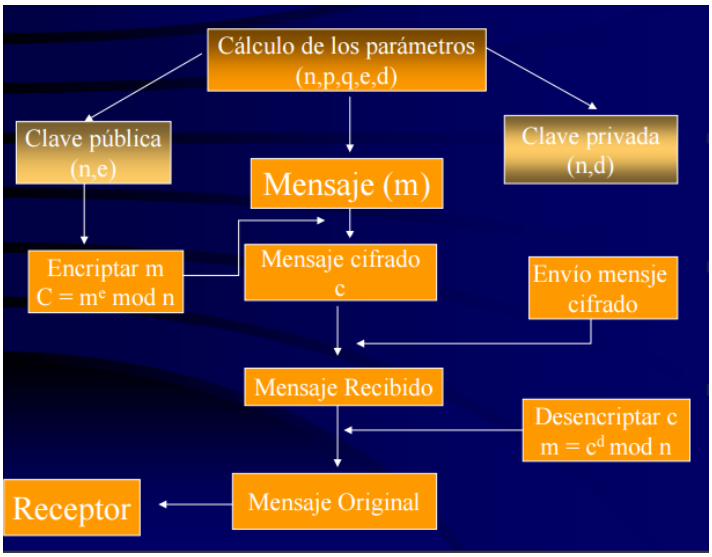


Fig.3. Funcionamiento del sistema RSA - Imagen tomada de: http://serdis.dis.ulpgc.es/~ii-cript/RSA.pdf

El cálculo de estas claves se realiza en secreto en la máquina en la que se va a guardar la clave privada, y una vez generada ésta conviene protegerla mediante un algoritmo criptográfico simétrico.

En cuanto a las longitudes de claves, el sistema RSA permite longitudes variables, siendo aconsejable actualmente el uso de claves de no menos de 1024 bits (se han roto claves de hasta 512 bits, aunque se necesitaron más de 5 meses y casi 300 ordenadores trabajando juntos para hacerlo).

De lo anterior el sistema RSA utiliza una función computacionalmente segura, ya que si bien realizar la exponenciación modular es fácil, su operación inversa para la extracción de raíces del módulo Ø, no es factible a menos que se conozca la factorización de e, correspondiente a la clave privada del sistema.
Cuanto mayor sea el tamaño del módulo mejor será la seguridad del sistema haciendo difícil el proceso de factorización mediante algún algoritmo para obtener los valores de "p" y "q", sin embargo el tamaño de la variable "n" influye negativamente en las operaciones del sistema RSA.

RSA es el más conocido y usado de los sistemas de clave pública, y también el más rápido de ellos. Presenta todas las ventajas de los sistemas asimétricos, incluyendo la firma digital, aunque resulta más útil a la hora de implementar la confidencialidad el uso de sistemas simétricos, por ser más rápidos. Se suele usar también en los sistemas mixtos para encriptar y enviar la clave simétrica que se usará posteriormente en la comunicación cifrada.

Hablando un poco de las aplicaciones actuales del sistema se deben tener en cuenta los aplicativos en instituciones bancarias, departamentos del gobierno de Estados Unidos, laboratorios nacionales, universidades, entre otros.

10. Servidores de Claves

Un servidor de claves es aquel que almacena llaves o claves públicas, de manera que se pueden buscar las claves públicas de una persona o usuario en el servidor mediante el nombre. Teniendo la llave pública se pueden dar usos como el cifrado de mensajes que se pueden enviar al dueño de la clave pública, comprobación de la firma digital de un mensaje enviado por el dueño de la clave pública.

Normalmente los servidores de claves suelen utilizarse por medio de correos electrónicos atendiendo peticiones de algún usuario, enviando el comando de solicitud de clave pública a un servidor (si existen varios conectados, se ponen en contacto entre ellos automáticamente y aquel servidor al que se envió el mail será el que conteste).

Algunos ejemplos de comandos de solicitud son:

- *ADD:* Añade una clave pública al servidor.
- *INDEX:* Muestra todas las claves públicas presentes en el servidor.
- *GET userid:* Obtiene la clave pública de un usuario.
- *MGET regexp:* Obtiene todas las claves públicas de los usuarios cuyo identificador concuerde con la expresión regular.
- *LAST hel:* Obtiene todas las claves públicas que fueron cambiadas en los últimos días.

Además de por correo electrónico, si el navegador usado soporta formularios, es posible obtener la información de los servidores de claves por medio de HTTP.
Algunos servidores de claves se pueden encontrar en la siguiente página WEB:

http://www.openpgp.net/pgpsrv.htm

11. Definición de PGP

Conocido también como Pretty Good Privacy (PGP), es una aplicación diseñada para proteger la información que se transmite a través de una red no asegurada; utilizando el método de criptografía hibrida (simétrica y asimétrica) para el cifrado y medio de transmisión de la información.

11.1. Funcionamiento

PGP es un cripto-sistema híbrido que combina técnicas de criptografía simétrica y criptografía asimétrica. Esta combinación permite aprovechar lo mejor de cada uno: El cifrado simétrico es más rápido que el asimétrico o de clave pública, mientras que éste, a su vez, proporciona una solución al problema de la distribución de claves en forma segura y garantiza el no repudio de los datos y la no suplantación.

Cuando un usuario emplea PGP para cifrar un texto en claro, dicho texto es comprimido. La compresión de los datos ahorra espacio en disco, tiempos de transmisión y, más importante aún, fortalece la seguridad criptográfica ya que la mayoría de las técnicas de criptoanálisis buscan

patrones presentes en el texto claro para romper el cifrado. La compresión reduce esos patrones en el texto claro, aumentando enormemente la resistencia al criptoanálisis.

Después de comprimir el texto, PGP crea una clave de sesión secreta que solo se empleará una vez. Esta clave es un número aleatorio generado a partir de los movimientos del ratón y las teclas que se pulsen durante unos segundos con el propósito específico de generar esta clave (el programa nos pedirá que los realicemos cuando sea necesario), también puede combinarlo con la clave anteriormente generada. Esta clave de sesión se usa con un algoritmo simétrico (IDEA, Triple DES) para cifrar el texto claro.

Una vez que los datos se encuentran cifrados, la clave de sesión se cifra con la clave pública del receptor (criptografía asimétrica) y se adjunta al texto cifrado, y el conjunto es enviado al receptor.
El descifrado sigue el proceso inverso. El receptor usa su clave privada para recuperar la clave de sesión, simétrica, que PGP luego usa para descifrar los datos.

Las claves empleadas en el cifrado asimétrico se guardan cifradas protegidas por contraseña en el disco duro. PGP guarda dichas claves en dos archivos separados llamados llaveros; uno para las claves públicas y otro para las claves privadas.

11.2. Aplicaciones de PGP

Las aplicaciones de PGP se resumen en programas de escritorio o móviles (repositorios y bases de datos) y aplicativos WEB, los cuales son usados para cifrar comunicaciones y archivos.
A continuación se mencionan los siguientes:

11.3. PGP Desktop

Esta aplicación es usada para cifrar correos electrónicos, datos en redes locales y discos duros.

11.4. GNUPG o GPG

Conocido también como Gnu Privacy Guard, es una herramienta disponible de forma gratuita y libre para varias plataformas incluyendo OS X a través de GPG Suite. En la página WEB se encuentran programas con entorno gráfico para usar GPG.

11.5. GPGshell

Es una aplicación usada por GNUPG para cifrar archivos, donde se pueden encontrar opciones como menús, ventanas y sin tener que usar la línea de comandos.

11.6. Enigmail

Esta aplicación es una extensión de Thunderbird y Seamonkey que permite cifrar mensajes de correo electrónico usando el estándar OpenPGP.

La aplicación permite crear claves distintas por cada cuenta de usuario, entre otras opciones.

11.7. GNUPGK

Es un programa basado en GNUPG utilizado para cifrar y des-cifrar toda clase de archivos. Ofrece soporte para PGP y tiene la forma para integrar en el menú contextual de Windows para ejecutar las acciones más sencillas directamente desde el botón derecho del mouse.

12. OpenPGP (Estándar RFC4880)

Se crea este estándar con el fin de publicar toda la información necesaria para la implementación y desarrollo de aplicaciones interoperables basados en el formato OpenPGP. En el documento se describe el formato y los métodos necesarios para leer, revisar, generar y escribir los paquetes que se transmiten por la red; sin ocuparse del almacenamiento y aplicación.

El Software OpenPGP utiliza una combinación de clave pública y criptografía simétrica para proporcionar servicios de seguridad para aplicativos en electrónica, comunicaciones y almacenamiento de datos. Estos servicios incluyen confidencialidad, gestión de claves, autenticación y digitales firmas. Este documento especifica los formatos de los mensajes utilizados en OpenPGP.

Dependiendo del software a trabajar se tendrán presentes las siguientes condiciones:

- *OpenPGP:* Este es un término para el software de seguridad que utiliza 5.x PGP como base, formalizado en RFC 2440 y RFC4880.
- *PGP (Pretty Good Privacy):* PGP es una familia de sistemas de software desarrollado por Philip R. Zimmermann de la que se basa OpenPGP.
- *2.6.x PGP:* Esta versión de PGP tiene muchas variantes, de ahí el termino PGP2.6.x. Se utiliza solo RSA, MD5, e IDEA por su tipo de criptografía transformada.
- *5.x PGP:* Esta versión de PGP se conocía anteriormente como "PGP 3" y también descrito en el predecesor de este documento RFC 1991. Cuenta con nuevos formatos y corrige una serie de problemas en el PGP diseño 2.6.x. Se la conoce aquí como 5.x PGP porque este software fue la primera versión de la base de código "PGP 3".
- *GnuPG - GNU Privacy Guard:* También llamada GPG-GnuPG es una aplicación de OpenPGP que evita todos los algoritmos gravados. En consecuencia, las primeras versiones de GnuPG no incluyeron llaves públicas RSA. GnuPG puede o no puede tener (según versión) el apoyo para IDEA u otros algoritmos gravados.

12.1. Funciones Generales

OpenPGP ofrece servicios de integridad de datos para los mensajes y archivos de datos mediante el uso de estas tecnologías básicas:

- Firmas digitales
- Cifrado
- Compresión
- Conversión Rdix-64

Además OpenPGP ofrece gestión de claves y servicios de certificado, pero muchos de ellos están más allá del alcance de este documento.

12.2. La confidencialidad mediante cifrado

OpenPGP combina el cifrado de clave simétrica y el cifrado de clave pública para proporcionar confidencialidad. Primero el objeto se cifra utilizando un algoritmo de cifrado simétrico. Cada llave simétrica se utiliza una sola vez, para un solo objeto. Una nueva "clave de sesión" es generada como un número aleatorio para cada objeto (a veces conocida como una sesión). Puesto que se utiliza una sola vez, la clave de sesión está ligada al mensaje y se transmite con él. Para proteger la clave, es cifrada con la clave pública del receptor.
La secuencia es la siguiente:

1. El emisor crea un mensaje.
2. El envío de OpenPGP genera un número aleatorio para ser usado como una clave de sesión por sólo este mensaje.
3. La clave de sesión se cifra con la clave pública de cada destinatario. Estas "claves de sesión cifrados" comienzan el mensaje.
4. El envío de OpenPGP cifra el mensaje utilizando la clave de sesión, que forma el resto del mensaje. Hay que tener en cuenta que el mensaje también se comprime.
5. El OpenPGP descifra la clave de sesión mediante la clave privada del destinatario.
6. El OpenPGP descifra el mensaje con la clave de sesión. Si el mensaje se comprime, se descomprime.

Con el cifrado de clave simétrica, un archivo puede ser encriptado con una clave simétrica derivada de una frase de contraseña (u otro secreto compartido), o un mecanismo de dos etapas similar al método de clave pública descrita anteriormente en el que una clave de sesión se cifra con un mismo algoritmo simétrico de encabezado de un secreto compartido.

Ambos de firma y de confidencialidad de servicios digitales se pueden aplicar al mismo mensaje. En primer lugar, una firma se genera para el mensaje y adjunto al mensaje. Entonces el mensaje, más la firma es encriptada usando una clave de sesión simétrica. Por último, la clave de sesión es cifrada mediante el cifrado de clave pública y el prefijo del cifrado bloque.

12.3. Autenticación a través de la firma digital

La firma digital utiliza un código hash o mensaje de “digerir algoritmo” (procesamiento de algoritmo), y un algoritmo de firma de clave pública.
La secuencia es la siguiente:

1. El emisor crea un mensaje.
2. El software de envío genera un código hash del mensaje.
3. El software de envío genera una firma del código hash utilizando la clave privada del remitente.
4. La firma binaria se adjunta al mensaje.
5. El software de recepción mantiene una copia de la firma del mensaje.
6. El software receptor genera un nuevo código hash del mensaje recibido y verifica el uso de la firma del mensaje. Si la verificación tiene éxito, el mensaje se acepta como auténtico.

12.4. Compresión

Las aplicaciones de OpenPGP deben comprimir el mensaje después de la aplicación de la firma pero antes del cifrado.

Si una aplicación no implementa la compresión, sus autores deben ser conscientes de que la mayoría de los mensajes OpenPGP en el mundo están comprimidos. Por lo tanto, incluso puede ser conveniente para un espacio con limitaciones de aplicación para aplicar la descompresión, pero no compresión.

Además, la compresión tiene el efecto secundario añadido de seguridad, que algunos tipos de ataques pueden ser frustrados por el hecho de estar comprimidos. Esto no es riguroso, pero es operacionalmente útil. Estos ataques pueden prevenirse mediante la aplicación y el uso de detección Modificación de códigos.

12.5. La conversión de Radix-64

Representación nativa subyacente de OpenPGP para los mensajes cifrados, certificados de firma y cerradura es una corriente de octetos arbitrarios.
Algunos sistemas sólo permiten el uso de bloques que consisten en siete bits, texto imprimible. Para el transporte de octetos binarios sin formato nativo de OpenPGP a través de canales que no son seguros para los datos binarios sin formato, una impresión es necesaria la codificación de estos octetos binarios. OpenPGP ofrece el servicio de convertir la corriente de octeto binario de 8 bits a un flujo de caracteres ASCII imprimibles, llamados Radix-64 codificación o ASCII Armor.

13. Servidores de claves PGP

Este tipo de servidores permite realizar las consultas y enviar los comandos tanto por mail como por protocolo HTTP, donde atiende peticiones múltiples mediante colas. Sin embargo, utiliza un sistema de gestión de base de datos propia, que permite tener varias bases de datos distintas (claves públicas).

Para un mejor aprovechamiento de los recursos de los servidores de claves PGP, se recomienda realizar la instalación de un servidor propio que se pueda adecuar a las necesidades de los usuarios. En algunos casos se puede sincronizar con el resto de servidores públicos para tener información tanto de la parte privada (servidor privado) y la parte pública (conexión con servidores públicos).

14. GNUPG

Es una aplicación completa y gratuita definido por el estándar RFC4880 (también conocido como PGP) del estándar OpenPGP la cual permite cifrar y firmar datos. Consta de un sistema de clave versátil es decir, que cuenta con diferentes módulos de acceso para todo tipo de clave pública. Este aplicativo también es conocido como GPG, el cual es una herramienta de línea de comandos con las características para una fácil integración con otras aplicaciones tales como MIME y Secure Shell (SSH).

Hablando un poco acerca de la forma en la que se distribuye GNUPG, es un software libre (significa que respeta su libertad) el cual puede ser usado libremente, modificado y distribuido bajo los términos de la licencia pública general de GNU.

El aplicativo tiene diferentes versiones como:

- *2.0.28:* Es el estable, versión sugerida para la mayoría de los usuarios.
- *2.1.6:* Esla versión moderna con soporte para ECC (Criptografía de variante elíptica, es una variación de la criptografía asimétrica) y muchas otras nuevas características.
- *1.4.19:* Es la versión clásica portátil.
- *GPG4WIN:* Es una versión de Windows de GNUPG estable, cuenta con un instalador y varias interfaces, en idiomas como Español, Inglés y Alemán.

En el aspecto técnico GNUPG ayuda no solo a encriptar la información, sino que también encripta y protege el medio en el cual se comunica (puertos del sistema).

15. Triple DES

Conocido también como 3DES o TDES, en criptografía es un tipo de algoritmo que realiza un triple cifrado tipo DES (Data Encryption Standard), lo cual incrementa la seguridad del cifrado de archivos DES simple.

Triple DES nació por la inseguridad que traía una clave de 56 bits. Las claves de 56 bits eran posibles de descifrar utilizando un ataque de fuerza bruta. El TDES agrandaba el largo de la llave, sin necesidad de cambiar de algoritmo cifrador.

El método de cifrado TDES desaparece progresivamente, siendo reemplazado por el algoritmo AES (Advanced Encryption Standard) que es considerado mucho más rápido (hasta 6 veces más rápido). De todas maneras, algunas tarjetas de créditos y otros métodos de pago electrónico, todavía tienen como estándar el algoritmo Triple DES.

Hablando acerca del funcionamiento de TDES es un algoritmo que funciona utilizando tres llaves en cada bloque de texto plano, en vez de utilizar una llave de 56 bits desde la tabla de llaves, TDES encripta el texto plano con la primera llave, luego encripta ese texto encriptado con otra llave de 56 bits, y por último encripta nuevamente el texto encriptado con otra llave de 56 bits.
Para explicar de mejor forma este proceso se debe tener en cuenta el siguiente orden:

- *Opción de codificación 1:* En este caso las tres claves son independientes, esta opción de codificación es la más fuerte, con 3 x 56 = 168 bits de la clave independiente.
- *Opción de codificación 2:* K1 y K2 son independientes, y K3 = K1, esta opción ofrece una menor seguridad, con 2 × 56 = 112 bits de la clave. Esta opción es más fuerte que la simple encriptación DES dos veces.
- *Opción de codificación 3:* Las tres claves son idénticas es decir K1 = K2 = K3, esta es equivalente a la DES, con sólo 56 bits de la clave. Esta opción proporciona compatibilidad con DES, porque las operaciones de primera y segunda se anulan.

Nota: K1, K2 Y K3 = Claves DES

Para descifrar este algoritmo, se tendrían que descubrir las tres llaves diferentes. No solo eso, el texto será des-encriptado solo cuando las tres llaves correctas sean usadas en el orden correcto. TDES también es capaz de trabajar con llaves más extensas para hacerlo más seguro.

En la siguiente imagen se muestra el proceso de cifrado del algoritmo TDES:

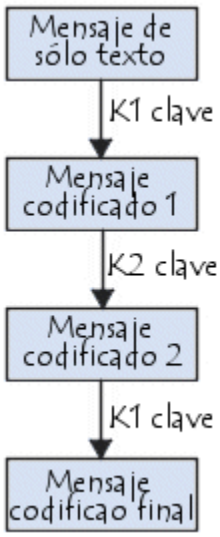


Fig.4. Proceso de cifrado TDES - Imagen tomada de: http://es.ccm.net/contents/130-introduccion-al-cifrado-mediante-des

El TDES permite aumentar de manera significativa la seguridad del DES, pero posee la desventaja de requerir más recursos para el cifrado y descifrado.

Por lo general, se reconocen diversos tipos de cifrado triple DES:

- *DES-EEE3:* Cifrado triple DES con 3 claves diferentes.

- *DES-EDE3:* Una clave diferente para cada una de las operaciones de triple DES (cifrado, descifrado, cifrado).

- *DES-EEE2 y DES-EDE2:* Una clave diferente para la segunda operación (descifrado).

En 1997, el NIST lanzó una nueva convocatoria para que desarrollar el AES (Advanced Encryption Standard, en castellano (Estándar de Cifrado Avanzado), un algoritmo de cifrado cuyo objetivo era reemplazar al DES.

El sistema de cifrado DES se actualizaba cada 5 años. En el año 2000, durante su última revisión y después de un proceso de evaluación que duró 3 años, el NIST seleccionó como nuevo estándar un algoritmo diseñado conjuntamente por dos candidatos belgas, el Sr. Vincent Rijmen y el Sr. Joan

Daemen. El nuevo algoritmo, llamado por sus inventores RIJNDAEL reemplazará, de ahora en adelante, al DES.

16. Firma Digital

Una firma digital es una transformación que por medio de una función relaciona de forma única un documento con la clave privada del firmante.

Actualmente existen diferentes tipos de firmas digitales como:

- Implícitas: Aquellas que están contenidas en el mensaje.
- Explícitas: Añadidas como una marca inseparable del mensaje.
- Privadas: Sólo pueden identificar al remitente aquellos quienes compartan una clave secreta con éste.
- Públicas (o verdaderas): Aquellas que gracias a información públicamente disponible cualquiera puede identificar al remitente.
- Revocables: En este caso el remitente puede negar que la firma le pertenece.
- Irrevocables: El receptor puede probar que el remitente escribió el mensaje.

La firma digital comprende dos procesos principales:

- *Firma:* (el firmante "A" crea una firma digital "s" para un mensaje "M"):

    1. Calcula s= sA(M), donde s es la firma de A sobre el mensaje M con la función de firma sA.
    2. Envía al receptor B la pareja (M,s).

- *Verificación*: (el receptor B verifica que la firma s sobre el mensaje M haya sido creada por "A".

    1. Obtiene la función de verificación VA de A.
    2. Calcula v= VA(M,s).
    3. Acepta la firma como creada por A si v= verdadero, y la rechaza si v= falso.

Las firmas digitales trabajan bajo el esquema de clave pública, en donde la clave privada se utiliza para firmar, y la pública para verificar la firma. Con el fin de evitar un ataque de hombre en medio, es aconsejable que se utilicen diferentes claves para el cifrado y para la firma digital.

Autenticación de identidad y de origen de datos, integridad y no repudio, son los servicios de seguridad que se proporcionan con el uso de firmas digitales.

En la práctica resulta poco eficiente firmar el documento completo, por lo que normalmente lo que se firma y envía es el hash del documento; en este caso tanto emisor como receptor deben acordar las funciones de firma y verificación.

17. Segmentación de redes

La segmentación de redes se originó a partir de algunos problemas ocasionados por el alto flujo del uso del internet, del cual podemos destacar el más importante que es la excesiva demanda de direcciones IP's y el agotamiento de las mismas.

Este término hace referencia a la división de una red en subredes para poder aumentar el número de ordenadores conectados a ella y mejorar el rendimiento teniendo en cuenta que solo se trabaja con un protocolo y un solo ambiente de trabajo.
La segmentación consiste en crear niveles de jerarquía en las direcciones IP's, generalmente se usan tres niveles (número de red, numero de subred y numero de estación), permitiendo así tener internamente un número ilimitado de direcciones IP internamente desde una dirección principal que externamente será transparente, es decir la estructura de la red no será visible.

Teniendo en cuenta este tema cabe aclarar sobre el concepto de segmento el cual es un bus lineal al que se conectan varias estaciones y tiene como características:

- Para interconectar varios segmentos se usan routers o switches.
- A cada segmento y estaciones conectadas se le llama subred.

Al dividirse una red o segmento, se auto gestiona de manera que la comunicación entre segmentos solo se realiza cuando es necesaria. La subred está trabajando por independiente. Por otro lado, el elemento que se utiliza para segmentar debe decidir a qué parte enviar la información (se usan repetidores, gateways, routers, entre otros).

Por último, es importante hablar de los protocolos de comunicación entre ordenadores.

18. Protocolo IPv4

Actualmente Internet está basada en el denominado Protocolo de Internet (IP, Internet Protocol), y desde su inicio comercial, se ha utilizado la versión 4 de dicho protocolo: "Internet Protocol version 4" (IPv4).

Este protocolo se diseñó prácticamente como un experimento, utilizando direcciones de 32 bits, con lo cual permite direccionar de forma única un máximo de 2 ^32 (4.294.967.296) dispositivos. Estas direcciones son las que se denominan direcciones IPv4 públicas. Una pequeña parte de este espacio de direcciones está destinado por IETF (Internet Engineering Task Force, la organización responsable de la estandarización de l os protocolos de Internet), para diversos servicios, como funciones de la red (multicast o m ultidifusión) y direcciones privadas (válidas sólo en el interior de las redes, pero no en Internet).
El despliegue inicial de Internet con IPv4 pasa por una fase inicial en la que se entregaban direcciones a cualquier persona o entidad que las solicitaba, sin mayores justificaciones.

19. Protocolo IPv6

En los últimos años, prácticamente desde que Internet tiene un uso comercial, la versión de este protocolo es el número 4 (IPv4).

Para que los dispositivos se conecten a la red, necesitan una dirección IP. Cuando se diseñó IPv4, casi como un experimento, no se pensó que pudiera tener tanto éxito comercial, y dado que sólo dispone de 2^32 direcciones (direcciones con una longitud de 32 bits, es decir, 4.294.967.296 direcciones), junto con el imparable crecimiento de usuarios y dispositivos, implica que en pocos meses estas direcciones se agotarán.

Por este motivo, y previendo la situación, el organismo que se encarga de la estandarización de los protocolos de Internet (IETF, Internet Engineering Task Force), ha trabajado en los últimos años en una nueva versión del Protocolo de Internet, concretamente la versión 6 (IPv6), que posee direcciones con una longitud de 128 bits, es decir 2^128 posibles direcciones (340.282.366.920.938.463.463.374.607.431.768.211.456).

El despliegue de IPv6 se irá realizando gradualmente, en una coexistencia ordenada con IPv4, al que irá desplazando a medida que dispositivos de cliente, equipos de red, aplicaciones, contenidos y servicios se vayan adaptando a la nueva versión del protocolo de Internet.

20. Firewall

Es un dispositivo que puede ser software o hardware sobre un sistema operativo, el cual sirve para filtrar el tráfico entre redes.
En general se podría considerar como una caja con DOS o más interfaces de red en la que se establecen una reglas de filtrado si una conexión decide establecerse o no. Actualmente un firewall es un hardware especifico con su sistema operativo que filtra el trafico TCP/UDP/ICMP/IP y decide si un paquete pasa, se modifica, se convierte o se descarta.

Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red. Esta sería la tipología clásica de un firewall:

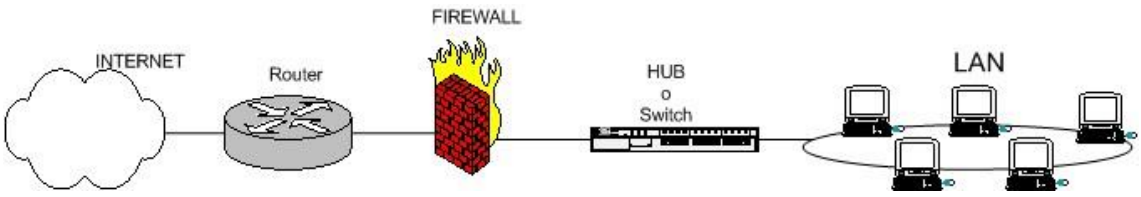


Fig.5. Esquema típico de firewall para proteger una red local conectada a internet a través de un router. - Imagen tomada de: http://www.pello.info/filez/firewall/iptables.html

En el esquema anterior el firewall debe colocarse entre el Router (conexión con un único cable) y la red local (conectado al Switch de la red LAN).
En una red pueden ponerse uno o más Firewall dependiendo de las necesidades de la red, para establecer distintos puntos de seguridad en torno a un sistema. Normalmente se necesita exponer

algún servidor a internet (como es el caso de un servidor web, un servidor de correo, etc.), y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos.
Lo que se recomienda en esa situación es situar ese servidor en un lugar aparte de la red, el que denominamos DMZ o zona desmilitarizada.

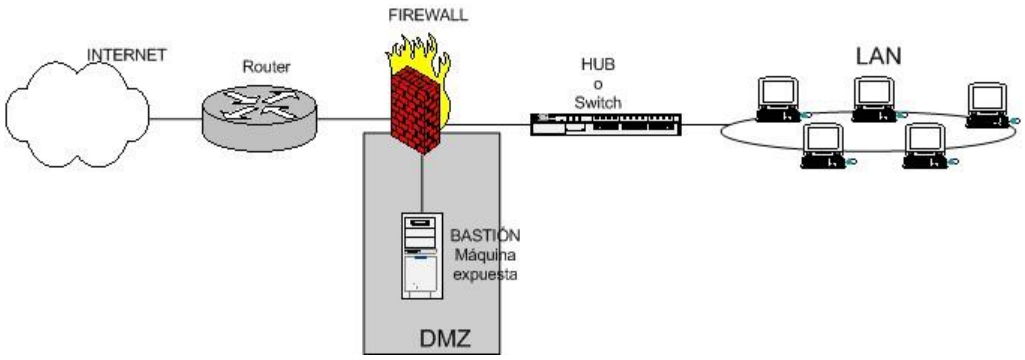


Fig.6. Esquema de firewall entre red local e internet con zona DMZ para servidores expuestos. - Imagen tomada de: http://www.pello.info/filez/firewall/iptables.html

Los firewalls se pueden usar en cualquier red. Es habitual tenerlos como protección de internet en las empresas, aunque ahí también suelen tener una doble función: controlar los accesos externos hacia dentro y también los internos hacia el exterior; esto último se hace con el firewall o frecuentemente con un proxy (que también utilizan reglas, aunque de más alto nivel).

21. IPTables

Es un sistema de firewall vinculado al kernel de Linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Al igual que el anterior sistema ipchains, un firewall de iptables no es como un servidor que lo iniciamos o detenemos o que se pueda caer por un error de programación (ha tenido alguna vulnerabilidad que permite DoS, pero nunca tendrá tanto peligro como las aplicaciones que escuchan en determinado puerto TCP), iptables está integrado con el kernel, es parte del sistema operativo.

Para hacerlo funcionar se deben aplicar reglas. Para ellos se ejecuta el comando iptables, con el que añadimos, borramos, o creamos reglas. Por ello un firewall de iptables no es sino un simple script de shell en el que se van ejecutando las reglas de firewall. En otras palabras IPTables permite crear reglas que analizarán los paquetes de datos que entran, salen o pasan por el ordenador, y en función de las condiciones que establezcamos, tomaremos una decisión que normalmente será permitir o denegar que dicho paquete siga su curso.

Para crear las reglas, podemos analizar muchos aspectos de los paquetes de datos. Podemos filtrar paquetes en función de:
Tipo de paquete de datos:

- Tipo INPUT: paquetes que llegan a nuestra máquina

- Tipo OUTPUT: paquetes que salen de nuestra máquina
- Tipo FORWARD: paquetes que pasan por nuestra máquina

Interfaz por la que entran (-i = input) o salen (-o = output) los paquetes

- eth0, eth1, wlan0, ppp0, ...

IP origen de los paquetes (-s = source):

- IP concreta
- Rango de red

IP destino de los paquetes (-d = destination):

- IP concreta
- Rango de red

Protocolo de los paquetes (-p = protocol):

- Tcp, udp, icmp...

Hacer NAT (modificar IP origen y destino para conectar nuestra red a otra red o a Internet):

- Filtrar antes de enrutar (PREROUTING).
- Filtrar después de enrutar (POSTROUTING).

Antes de involucrar en nuestro contenido el marco legal y normas que regulan las condiciones para la preservación digital y los repositorios digitales, es necesario dejar claro el concepto de metadato.

22. Metadato

Los metadatos son información estructurada o semi-estructurada que posibilita la creación, registro, clasificación, acceso, conservación y disposición de los documentos a lo largo del tiempo y dentro de un mismo dominio o entre dominios diferentes. Cada uno de estos dominios, representa un área del discurso intelectual y de la actividad social o de la organización, desarrollado por un grupo propio o limitado de individuos que comparten ciertos valores y conocimiento. Los metadatos para la gestión de documentos pueden usarse para identificar, autenticar y contextualizar tanto los documentos como los agentes, procesos y sistemas que los crean, gestionan, mantienen y utilizan, así como las políticas que los rigen.

Inicialmente, los metadatos definen el documento en el mismo momento de su incorporación, fijándole en su contexto y estableciendo el control de su gestión. Durante la existencia de los documentos o sus agrupaciones, se irán añadiendo nuevas capas de metadatos debido a la existencia de nuevos usos en otros contextos. Esto significa que a lo largo del tiempo los metadatos continúan acumulando información relacionada con el contexto de gestión de los documentos, los procesos de negocio en los que se utilizan, así como sobre los cambios estructurales que les afectan o su

apariencia. Los metadatos aplicados a los documentos durante su vida activa pueden también seguir utilizándose cuando no sean necesarios para la gestión pero sean conservados para facilitar la investigación o debido a otros valores Los metadatos aseguran la autenticidad, la fiabilidad, la disponibilidad y la integridad de los objetos de información a lo largo del tiempo, ya sean éstos físicos, analógicos o digitales, y posibilitan su gestión y comprensión. Sin embargo, también es necesario gestionar los metadatos.

La gestión de los documentos siempre ha implicado la gestión de los metadatos. No obstante, el entorno digital precisa una expresión diferente de los requisitos tradicionales, y unos mecanismos distintos para la identificación, incorporación al sistema, asignación y uso de los metadatos. En el entorno digital, los documentos autorizados son aquellos que se acompañan de metadatos que definen sus características fundamentales. Estas características deben estar explícitamente documentadas, y no de manera implícita como en algunos procesos basados en papel. En el entorno digital, es esencial asegurar que las funciones de creación e incorporación de metadatos estén implantadas en los sistemas que crean, incorporan y gestionan documentos. Inversamente, el entorno digital presenta nuevas oportunidades para definir y crear metadatos y asegurar la incorporación completa y actualizada de documentos al sistema. Estos documentos pueden ser testimonio de operaciones o constituirlas ellos mismos [15].

Por otro lado se debe tener en cuenta el marco legal o normas que regulan las condiciones para la preservación digital y los repositorios digitales, por tal motivo se dará a conocer la siguiente norma ISO:

23. Información y documentación - Procesos de gestión de documentos - Metadatos para la gestión de documentos. Parte 1: Principios. ISO 23081-1:2006

ISO 23081 establece un marco para la creación, gestión y uso de metadatos para la gestión de documentos, y explica los principios por los que deben regirse. La Norma ISO 23081 es un guía para entender, implantar y utilizar metadatos en el marco de la Norma ISO 15489, Información y documentación-Gestión de documentos. Trata de la importancia de los metadatos propios de la gestión de documentos en los procesos de negocio, de los diferentes tipos de metadatos y del papel que desempeñan tanto para los propios procesos de trabajo como para los procesos de gestión de documentos. También establece el marco para gestionar estos metadatos. No define un conjunto obligatorio de metadatos para la gestión de documentos, ya que estos diferirán en el detalle según los requisitos específicos de cada organización u ordenamiento jurídico. Sin embargo, sirve para evaluar los principales conjuntos de metadatos existentes contrastándolos con los requisitos de ISO 15489. Esta parte de la ISO 23081 establece un marco para la creación, gestión y uso de metadatos para la gestión de documentos, y explica los principios por los que deben regirse [16].
El campo de aplicación de la norma ISO 23081 aborda los principios que sustentan y rigen los metadatos para la gestión de documentos. Dichos principios se aplican a lo largo del tiempo a:

- Los documentos y sus metadatos
- Todos los procesos que les afectan
- Cualquier sistema en el que residan
- Cualquier organización responsable de su gestión

Capítulo III

Diseño y Desarrollo del proyecto

Para el diseño y desarrollo del repositorio con seguridad planteado en este proyecto, se tuvieron en cuenta las variables presentadas a continuación fundamentadas teóricamente gracias a la información del marco teórico. Se ha considerado en cada etapa planteada y desarrollada, cumplir con los requerimientos propuestos a lo largo de los objetivos del trabajo. A continuación se presenta la metodología empleada para cada una de las etapas y procesos tomados para llevar a cabo su desarrollo.

Variables

24.1. Variables Directas

Repositorio de archivos, información (archivos de la empresa), medio de transmisión de la información.

24.2. Variables Indirectas

Repositorio de llaves públicas, llaves públicas, llaves privadas.

24.3. Variables Independientes

Desorganización de información, Inseguridad en la información, inseguridad en el medio de transmisión de la información.

24.4. Variables Dependientes

Organización de la información, seguridad en el medio de transmisión de la información, seguridad de la información, privacidad de la información entre departamentos.

Diseño Metodológico

25.1. Diseño metodológico del Experimento

Teniendo en cuenta la explicación de cada uno de los procesos requeridos para la implementación del repositorio con seguridad descritos anteriormente, es necesario dar a conocer los elementos y herramientas necesarias que conllevaron al desarrollo y funcionamiento del proyecto.

El objeto de este proyecto está enfocado en la implementación de un repositorio con seguridad que garantice el orden, control, privacidad y seguridad de la información de la empresa.

Materiales:

- Computador con los siguientes requerimientos mínimos (Procesador: Intel Quad Core, Memoria Instalada (RAM): 4,0 GB, Sistema Operativo: 32 Bits o 64 bits)
- Instalador del software libre VirtualBox (cualquier versión)
- Instalador del software libre Kleopatra (cualquier versión)
- Instalador del software libre PSFTP (cualquier versión)
- Imagen ISO Windows XP 64 bits o 32 bits
- Imagen ISO Ubuntu Linux 14.04.2
- Imagen ISO Ubuntu Server 14.04.2

Cabe aclarar que en el manual donde se describen los procedimientos para la implementación del repositorio con seguridad, no hace mención de las técnicas de recolección de información de la empresa. Por tal motivo en el manual se realiza el procedimiento completo con dos tipos de archivos (archivo de texto (.txt) y archivo de imagen (.jpg)) a manera de ejemplo, los cuales dan a entender que se puede realizar con cualquier tipo de archivo.

El desarrollo completo del proyecto se describe en el manual (Anexo D).

Desarrollo del repositorio con seguridad

El repositorio con seguridad está conformado por las siguientes etapas, teniendo en cuenta el manual de implementación del repositorio con seguridad descrito en los anexos (parte final del trabajo):

26.1. Instalación del software virtualizador VIRTUAL BOX

26.2. Montaje de máquinas virtuales (Windows XP, Linux, Ubuntu Server SSH o Ubuntu Server Keys).

26.3. Instalación del paquete OPENSSH en Ubuntu Server SSH

26.4. Prueba de comunicación entre máquinas virtuales con el servidor

26.5. Creación de grupos, usuarios y carpetas en el servidor

26.6. Instalación del paquete SKS-KEYSERVER (OPENPGP) en Ubuntu Server Keys

26.7. Creación de llaves pública y privada (para el proceso de encriptación y des-encriptación de archivos)

26.8. Almacenamiento de llaves públicas desde el usuario al servidor Ubuntu Server Keys

26.9. Encriptación y almacenamiento de archivos en el repositorio Ubuntu Server SSH.

26.10. Descarga y des-encriptación de archivos del repositorio Ubuntu Server SSH a los usuarios Linux (Departamento de Operaciones)

26.11. Instalación de la aplicación GPG4WIN (Software libre Kleopatra)

26.12. Creación de llaves pública y privada (para el proceso de encriptación y des-encriptación de archivos para usuarios XP) con el Software Kleopatra

26.13. Almacenamiento de llave pública desde el usuario al Servidor Ubuntu Server Keys (para usuarios Windows xp1 y xp2)

26.14. Proceso de encriptación de archivos y almacenamiento de archivos en el repositorio Ubuntu Server SSH (Para usuarios XP)

26.14.1. Proceso de Encriptación

26.14.2. Proceso de almacenamiento de archivos en el repositorio Ubuntu Server SSH

26.15. Proceso de descarga y des-encriptación de archivos del repositorio Ubuntu Server SSH a los usuarios XP (Departamento de Ventas y Finanzas)

26.15.1. Proceso de descarga de archivos desde el repositorio Ubuntu Server SSH a los usuarios XP (Departamentos de Ventas y Finanzas)

26.15.2. Proceso de des-encriptación de archivos del repositorio Ubuntu Server SSH a los usuarios XP1 o XP2 (Departamentos de Ventas y Finanzas)

26.16. Enjaulado de Usuarios.

26.17. Instalación de IPTABLES (FIREWALL).

Partiendo de la necesidad de implementar una solución al problema de la seguridad de archivos entre los departamentos de la empresa, se decide implementar una aplicación como resultado del conjunto de la instalación y uso de diversos software libres en los computadores de la empresa.
Por tal motivo el proyecto se manejará en su totalidad por software.

26.1. Instalación del software virtualizador VIRTUAL BOX

Para comenzar la implementación del repositorio con seguridad es necesario tener presente el computador o equipo físico en el cual se instalarán los programas y aplicaciones que lo componen. Para ello se tendrán presentes las características de sistema, como se describen a continuación:

- Procesador: Intel Quad Core
- Memoria Instalada (RAM): 8,0GB
- Tipo de Sistema: Sistema Operativo de 64 bits

Con lo anterior se podrá instalar VirtualBox, el programa principal en el que se implementará el repositorio con seguridad.

Virtual Box es un software de virtualización para arquitecturas x86 que fue desarrollado originalmente por la empresa alemana Innotek GmbH, pero que pasó a ser propiedad de la empresa Sun Microsystems en febrero de 2008 cuando ésta compró a innotek. Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como "sistemas invitados", dentro de otro sistema operativo "anfitrión", cada uno con su propio ambiente virtual. Por ejemplo, se podrían instalar diferentes distribuciones de GNU/Linux en VirtualBox instalado en Windows XP o viceversa.

Entre los sistemas operativos soportados (en modo anfitrión) se encuentran GNU/Linux, Mac OS X, OS/2 Warp , Windows, y Solaris/OpenSolaris, y dentro de éstos es posible virtualizar los sistemas operativos FreeBSD, GNU/Linux, OpenBSD, OS/2 Warp, Windows, Solaris, MS-DOS y muchos otros.
En comparación con otras aplicaciones privadas de virtualización, como VMware Workstation o Microsoft Virtual PC, VirtualBox carece de algunas funcionalidades, pero provee de otras como la ejecución de máquinas virtuales de forma remota, por medio del Remote Desktop Protocol (RDP), soporte iSCSI.

En cuanto a la emulación de hardware, los discos duros de los sistemas invitados son almacenados en los sistemas anfitriones como archivos individuales en un contenedor llamado Virtual Disk Image, incompatible con los demás software de virtualización.

Otra de las funciones que presenta es la de montar imágenes ISO como unidades virtuales de CD o DVD, o como un disco floppy. [20]

Partiendo de la información anterior se procede a realizar el proceso de instalación del software virtualizador Virtual Box, teniendo en cuenta los pasos descritos en el manual.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 6 a la 11).

26.2. Montaje de máquinas virtuales (Windows XP, Linux, Ubuntu Server SSH o Ubuntu Server Keys)

Teniendo instalado el software libre de virtualización instalado en el equipo, ahora se pueden instalar (montar) las siguientes máquinas virtuales que representan los departamentos de la empresa, el repositorio con seguridad y el servidor de llaves públicas con sus respectivos sistemas operativos, tal como se describen a continuación:

- Ubuntu Server SSH (Repositorio con seguridad - Ubuntu Server 14.04.2)
- Ubuntu Server Keys (Repositorio de llaves públicas – Ubuntu Server 14.04.2)
- Windows XP1 (Departamento de Ventas – Windows Xp de 64 Bits)
- Windows XP2 (Departamento de Finanzas – Windows Xp de 64 Bits)
- Linux (Departamento de Operaciones – Ubuntu Desktop 14.04.2)

En el montaje de las máquinas virtuales se debe tener en cuenta el espacio de almacenamiento propio de cada sistema operativo y su menoría RAM.

Teniendo presente la información anterior se procede a realizar el proceso de montaje de las máquinas virtuales, tal como se describe en los pasos del manual.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 12 a la 17).

26.3. Instalación del paquete OPENSSH en Ubuntu Server SSH

Una vez montadas las máquinas virtuales en el software libre de virtualización Virtual Box, es necesario instalar el paquete OpenSSH para el repositorio con seguridad Ubuntu Server SSH, ya que permite la conexión segura de los usuarios para los procesos de carga y descarga de información (archivos).

Para este proceso es necesario seguir los pasos del manual, ingresando en orden los comandos en la consola de Ubuntu Server SSH (Repositorio con seguridad).

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Ingresar los comandos en consola de acuerdo al orden establecido en los pasos).

26.4. Prueba de comunicación entre máquinas virtuales con el servidor

Un aspecto importante en la implementación del proyecto es la comunicación entre las máquinas virtuales, ya que sin esta no se podrá realizar la transferencia de archivos entre los departamentos de la empresa y los repositorios.

De lo anterior, ahora se asignan direcciones IP fijas a cada máquina virtual para que se identifiquen y diferencien entre sí, de esta manera se verifica la comunicación entre ellas mediante el comando "Ping (dirección)" que comprueba el estado de la comunicación del Host Local (Departamento o repositorio) con uno o varios equipos remotos de la red IP por medio del envío y recepción de paquetes.

En el Anexo A (Diagrama de comunicación entre máquinas virtuales) se describe la forma en la que debe realizarse la prueba de comunicación entre los Departamentos de la empresa y los Repositorios.

Teniendo presente la información anterior se procede a realizar el proceso de prueba de comunicación entre máquinas virtuales con los servidores, tal como se describe en los pasos del manual.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 18 a la 36).

26.5. Creación de grupos, usuarios y carpetas en el servidor

El siguiente procedimiento se realiza en las máquinas virtuales de los Departamentos de la empresa y principalmente en el repositorio con seguridad (Ubuntu Server SSH), para organizar tanto los usuarios de la empresa como la información (archivos) de interés de cada uno.

Para comenzar se crean los grupos los cuales van a tener una cierta cantidad de usuarios y unas carpetas determinadas, tal como se puede visualizar en los pasos descritos en el manual.
Los grupos para la empresa serán los siguientes:

- Operaciones

- Ventas
- Finanzas

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 37 a la 39).

Ahora se crean los usuarios los cuales van a manipular directamente la información de la empresa (archivos), como se describe en los pasos del manual.
Los usuarios de la empresa son los siguientes:

- Phernandez
- Caponte
- Apinillos
- Mleon
- Hleon
- Fbernal
- Fsanchez
- Mbarranco
- gleon

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 40 a la 46).

A continuación se procede a crear las carpetas donde se almacenará la información (archivos) en el repositorio con seguridad, como se puede visualizar en los pasos del manual.
Cabe aclarar que el proyecto se desarrolla teniendo en cuenta que el Departamento de Ventas y Finanzas están compartiendo archivos y carpetas, mientras que el Departamento de Operaciones no comparte información con ningún otro.
Las carpetas tienen el mismo nombre que los grupos para una fácil identificación de los usuarios para su respectivo acceso, las carpetas son las siguientes:

- Operaciones
- Ventas
- Finanzas

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 47 a la 48).

Ya teniendo creados los grupos, usuarios y carpetas lo último que se hace es vincular cada uno de los usuarios a los respectivos grupos y de igual manera estos a las carpetas del repositorio, como se puede observar en los pasos del manual.

Nota: Revisar el *Anexo E. Tabla de contraseñas de los usuarios (Departamentos de Operaciones, Ventas y Finanzas),* para visualizar de mejor forma el proceso de vinculación de usuarios a grupos.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 49 a la 50).

26.6. Instalación del paquete SKS-KEYSERVER (OPENPGP) en Ubuntu Server Keys

Para complementar la implementación de este proyecto es necesario instalar el servidor de llaves públicas (Ubuntu Server Keys), ya que permitirá desarrollar el proceso de encriptación y des-encriptación de información (archivos) de los departamentos de la empresa para blindarles seguridad y privacidad.

Partiendo de lo anterior, se debe instalar el servidor SKS-KEYSERVER que es un servidor OPENPGP, cuya función es la sincronización de llaves públicas de manera sencilla, descentralizada y confiable.

Teniendo presente la información anterior se procede a realizar el proceso de instalación del paquete SKS-KEYSERVER (OPEN PGP) en la máquina virtual Ubuntu Server Keys, tal como se describe en los pasos del manual.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 51 a la 57).

26.7. Creación de llaves pública y privada (para el proceso de encriptación y des-encriptación de archivos)

Para este proceso es necesario diferenciar los dos sistemas operativo que se manejarán en el proyecto, Windows XP (Departamentos de Ventas y Finanzas) y Ubuntu Linux (Departamento de Operaciones) ya que se manejará la generación de llaves públicas y privadas que son necesarias para el proceso de encriptación y des-encriptación de archivos que brinda mayor seguridad en el manejo y manipulación de archivos, tal como se describe en el concepto criptografía asimétrica y el sistema de seguridad RSA.

Teniendo presente la información anterior y los pasos descritos en el manual de implementación del repositorio con seguridad, en la máquina virtual Linux correspondiente al departamento de operaciones se pueden realizar dos procesos de generación de llaves públicas y privadas. Uno de ellos mediante la aplicación “Contraseñas y Claves” tal como se indica en el manual de la forma gráfica o más versátil para los usuarios.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 58 a la 62).

Por otro lado se tiene el proceso de generación de llaves por ingreso de comandos en la consola del sistema operativo, como se indica en las imágenes del manual del repositorio con seguridad.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 63 a la 73).

26.8. Almacenamiento de llaves públicas desde el usuario al servidor Ubuntu Server Keys

Este procedimiento se realiza con el fin de garantizar el orden de las llaves públicas, ya que para realizar el proceso de encriptación (definición de criptografía asimétrica) es necesario tener la llave pública del usuario que desea ver la información, para poder encriptarla y con su respectiva llave privada se des-encripta.

Como ya se había mencionado anteriormente, este procedimiento se realiza de dos maneras diferentes dependiendo del sistema operativo que se maneje ya sea Windows XP (Departamentos de Ventas y Finanzas) o Linux (Departamento de Operaciones). Para dar continuidad con los pasos del manual, primero se tendrá en cuenta para Linux.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 74 a la 75).

26.9. Encriptación y almacenamiento de archivos en el repositorio Ubuntu Server SSH

Esta etapa del proyecto es fundamental ya que entra en funcionamiento el repositorio con seguridad en el almacenamiento y descarga de información (archivos de la empresa).
Teniendo presente el orden del manual de implementación del repositorio, se desarrollará este proceso para Linux (Departamento de Operaciones).

A manera de visualización del proceso, se realizará el ejemplo con un archivo de texto plano sin embargo se puede realizar con cualquier tipo de archivo pero los tiempos de encriptación y almacenamiento de archivos al repositorio con seguridad Ubuntu Server SSH aumentarán o disminuirán dependiendo del tamaño y tipo de archivo.
Teniendo presente la información del marco teórico con respecto a la criptografía asimétrica, es necesario descargar la llave pública del usuario que desea ver el contenido real del archivo para que cuando el archivo este encriptado, se pueda almacenar en el repositorio tal como se propone en los pasos del manual de implementación del repositorio con seguridad.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 76 a la 85).

26.10. Descarga y des-encriptación de archivos del repositorio Ubuntu Server SSH a los usuarios Linux (Departamento de Operaciones)

Este proceso de descarga y des-encriptación de archivos se realiza para culminar con el proceso definido en la criptografía asimétrica.

Conociendo el nombre del archivo encriptado, al ingresar remotamente al repositorio con seguridad Ubuntu Server SSH se realiza el proceso de descarga al usuario que desea ver la información para que luego con su llave privada se pueda des-encriptar el archivo descargado y observar la información de interés.

El proceso se realiza de acuerdo al orden de los pasos del manual.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 86 a la 90).

Hasta este punto del proyecto se ha desarrollado de acuerdo a la definición de la criptografía asimétrica, garantizando la seguridad del medio de transmisión de la información y los archivos de la empresa en el sistema operativo Linux.

En los siguientes pasos se describirá el proceso de criptografía asimétrica utilizando las diversas herramientas con el sistema operativo Windows XP.

26.11. Instalación de la aplicación GPG4WIN (Software libre Kleopatra)

Para el sistema operativo Windows XP, no se cuenta con una serie de comandos o herramientas integradas para realizar el proceso de criptografía asimétrica, por tal motivo se requiere de programas o software libre que permita realizar las funciones de generación de llaves públicas y privadas, encriptación y des-encriptación de archivos y almacenamiento de los usuarios de los Departamentos de Ventas y Finanzas al repositorio con seguridad Ubuntu Server SSH.

Teniendo en cuenta lo anterior, es necesario instalar la aplicación GPG4WIN que contiene el software libre Kleopatra el cual es una herramienta utilizada para el cifrado y des-cifrado de correo electrónico y archivos para la mayoría de las versiones de Microsoft Windows que utiliza GNUPG (Criptografía de llave pública). [21]

Este proceso se desarrolla según los pasos descritos en el manual.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 91 a la 101).

26.12. Creación de llaves pública y privada (para el proceso de encriptación y des-encriptación de archivos para usuarios XP) con el Software Kleopatra

El software libre Kleopatra permite crear las llaves públicas y privadas de los usuarios del sistema operativo Windows XP necesarias para encriptar y des-encriptar archivos, de una manera muy sencilla y versátil a comparación del sistema operativo Linux.

A continuación se describirá el proceso de generación de las llaves públicas y privadas para encriptar y des-encriptar los archivos manejados en los departamentos de Ventas y Finanzas, siguiendo la secuencia de los pasos descritos en el manual.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 102 a la 110).

26.13. Almacenamiento de llave pública desde el usuario al Servidor Ubuntu Server Keys (para usuarios Windows xp1 y xp2)

El proceso de almacenamiento de llaves públicas de los usuarios de los Departamentos de Ventas y Finanzas en el servidor Ubuntu Server Keys es similar al realizado en el sistema operativo Linux, la única diferencia está en la asignación de la información de la transferencia de la llave al repositorio como dirección IP del servidor, puerto de comunicación con el servidor, modo de conexión con el servidor, entre otros.

Teniendo las llaves públicas y privadas generadas, ahora se almacenan las llaves públicas en el servidor Ubuntu Server Keys para el proceso de encriptación de archivos, tal como se indica en el manual.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 111 a la 115).

26.14. Proceso de encriptación de archivos y almacenamiento de archivos en el repositorio Ubuntu Server SSH (Para usuarios XP)

En esta parte del proyecto se tienen en cuenta dos procesos importantes en el desarrollo del proyecto, donde también se tiene en cuenta como con el sistema operativo Linux.

26.14.1. Proceso de Encriptación

Para el proceso de encriptación se debe tener en cuenta el mismo procedimiento realizado para los usuarios Linux (Departamento de Operaciones), pero en este caso se desarrollará el ejemplo con un archivo de imagen (.jpg).

La diferencia de Windows Xp (Departamentos de Ventas y Finanzas) y Linux (Departamento de Operaciones) está en la forma en que se desarrolla el procedimiento. Como se observará en las imágenes y la secuencia de los pasos del manual, tan solo con hacer click derecho con el mouse sobre el archivo a trabajar el software libre Kleopatra empieza a actuar.

Hablando acerca del proceso de encriptación, es necesario descargar la llave pública del usuario que desea ver la información cifrada donde el mismo programa ofrecerá la opción de selección de la llave pública con la que se desea realizar el procedimiento.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 116 a la 129).

26.14.2. Proceso de almacenamiento de archivos en el repositorio Ubuntu Server SSH:

Como en el caso del sistema operativo Linux (Departamento de Operaciones), una vez encriptado el archivo en este caso la imagen "Sunset.jpg.gpg" se realiza el proceso de almacenamiento del archivo en el repositorio Ubuntu Server SSH, con la ayuda del programa libre ejecutable (Psftp.exe) el cual es una herramienta para la transferencia de archivos de forma segura entre ordenadores utilizando la conexión SSH para brindar más seguridad.

Teniendo presente lo anterior, se desarrolla el procedimiento de acuerdo a la secuencia de pasos del manual.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 130 a la 136).

26.15. Proceso de descarga y des-encriptación de archivos del repositorio Ubuntu Server SSH a los usuarios XP (Departamento de Ventas y Finanzas)

Cabe aclarar que para desarrollar este proceso se debe tener presente el usuario que desea ver la información encriptada, ya que según el proceso de encriptación asimétrica sólo se puede des-encriptar la información mediante la llave privada del usuario.
Para el caso del ejemplo, el archivo de imagen "Sunset.jpg" fue encriptado con la llave pública del usuario "mbarranco" el cuál des-encriptará la información del archivo "Sunset.jpg.gpg" con la llave privada que sólo este usuario posee.

25.15.1 Proceso de descarga de archivos desde el repositorio Ubuntu Server SSH a los usuarios XP (Departamentos de Ventas y Finanzas)

Teniendo presente lo anterior, el usuario "mbarranco" del Departamento de Finanzas debe ingresar remotamente al repositorio con seguridad Ubuntu Server SSH donde realizará la descarga del archivo encriptado con su llave pública, asignando en el programa libre ejecutable (Psftp.exe) la ubicación donde desea almacenar el archivo.

Se debe realizar este procedimiento teniendo en cuenta la secuencia de los pasos del manual.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 137 a la 143).

25.15.2. Proceso de des-encriptación de archivos del repositorio Ubuntu Server SSH a los usuarios XP1 o XP2 (Departamentos de Ventas y Finanzas):

Para el proceso de des-encriptación es necesario tener la llave privada del usuario que desea ver la información, para este caso el usuario del departamento de finanzas "mbarranco" puede realizar el proceso de des-encriptación ya que el archivo "Sunset.jpg.gpg" fue encriptado con su llave pública.

En el manual se explica de forma detallada el proceso desarrollado con su respectiva verificación.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 144 a la 149).

Hasta este punto del proyecto se ha desarrollado y cumplido lo propuesto en los objetivos del proyecto, sin embargo quedan dos detalles de vital importancia como lo son el enjaulado de usuarios y la instalación del firewall.

26.16. Enjaulado de Usuarios

El enjaulado de usuarios consiste en re-configurar el archivo del repositorio con seguridad "sshd_config", asignando el grupo y ubicación de la carpeta dentro del repositorio a donde se requiere buscar la información del Departamento. El funcionamiento se visualiza cuando cualquiera de los usuarios de la empresa al ingresar remotamente al repositorio con seguridad, ingresa directamente a los archivos de la carpeta del Departamento al que pertenezca.

Este proceso garantiza la privacidad y exclusividad de las carpetas de los Departamentos de la empresa.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 150 a la 158).

26.17. Instalación de IPTABLES (FIREWALL)

Teniendo en cuenta que hasta esta etapa del manual el proyecto está realizado en su totalidad, sin embargo es recomendable brindar al repositorio con seguridad Ubuntu Server SSH mayor seguridad de ingreso de manera que solo la empresa tenga acceso al mismo y ningún computador externo pueda acceder al repositorio, así tenga conocimiento de la dirección IP del mismo.

Por tal motivo se instala el firewall (IPTABLES) para garantizar la seguridad de la información de los usuarios de los diferentes departamentos de la empresa en cuanto a la transferencia de archivos, mediante la asignación de reglas permitiendo el filtrado del tráfico de red.

La instalación del firewall se realiza teniendo en cuenta los pasos descritos en el manual.

Nota: Revisar el *Anexo D. Manual de Implementación del repositorio con Seguridad* (Figuras 159 a la 161).

Capítulo IV

Resultados

Tal como se empezó a desarrollar en el capítulo anterior, los resultados se presentarán en el orden en el que se implementó el repositorio con seguridad bajo la descripción del manual.
Cabe aclarar que en el manual se tuvieron en cuenta los procedimientos de instalación de los software libre (VirtualBox y Kleopatra), instalación de las máquinas virtuales, comunicación entre ellas, instalación del paquete OPENSSH, etc. Sin embargo en este capítulo no se presentarán resultados finales de estos ya que los resultados de vital importancia están relacionados con los procesos de seguridad del medio de transmisión de la información (archivos), encriptación y des-encriptación de archivos.

27.1. Creación de llaves pública y privada (para el proceso de encriptación y des-encriptación de archivos)

Partiendo de la explicación del capítulo anterior y haciendo relación a este proceso (26.7.), en el sistema operativo Linux (Departamento de Operaciones) se tiene dos procesos diferentes para la generación de llaves públicas y privadas.

27.1.1. Creación de llaves pública y privada con GNUPG (Modo gráfico de generación de llaves)

La aplicación de este método fue bastante entendible para el usuario al momento de su manipulación, ya que de forma gráfica se presentaron los requerimientos necesarios para la creación de las llaves pública y privada.
Hay que tener en cuenta que en el desarrollo del manual se visualiza el procedimiento para uno de los usuarios, que de igual forma se realiza para los dos restantes.

En la imagen correspondiente a la verificación del procedimiento, se puede observar el resultado de la creación de las llaves pública y privada como consecuencia de la aplicación de los pasos del manual.

Nota: Revisar Imagen (*Fig.62. Verificación de las llaves pública y privada creadas en la aplicación Contraseñas y claves desde el usuario Linux (Departamento de Operaciones)*)

27.1.2. Creación de llaves pública y privada con GNUPG (Generación de las llaves por consola)

Mediante este método se puede realizar la creación de llaves pública y privada, sin embargo es un procedimiento más complejo ya que necesita del ingreso de comandos por parte del usuario de manera sencilla pero extensa.

Por otro lado se debe tener presente que este método requiere de bastante tiempo ya que para la creación de las llaves pública y privada, se necesita la generación de entropía (cantidad de información promedio que contienen los símbolos usado) para que el sistema obtenga bytes aleatorios y así pueda crear las llaves con mayor seguridad. Todo esto depende del tamaño de llaves que se desee crear, para el caso del proyecto se crearán llaves de 20148 bits.

Los resultados del proceso descritos anteriormente, se pueden visualizar en las imágenes del manual que se tiene como resultado de la creación de las llaves pública y privada bajo la comprobación por el comando "seahorse" en la consola y la visualización en la aplicación "Contraseñas y claves" por el método gráfico.

Nota: Revisar imágenes (*Fig.69. a la Fig.73.*)

27.2. Almacenamiento de llaves públicas desde el usuario Linux (departamento de operaciones) al servidor Ubuntu Server Keys

Para el desarrollo de este proceso tan solo basta con ingresar en la consola del usuario Linux (Departamento de Operaciones) los comandos tal como se describe en los pasos del manual (Fig.74 y Fig.75).

En la imagen de la verificación del almacenamiento de llaves públicas al servidor Ubuntu Server Keys se podrá observar el resultado para uno de los usuarios del departamento de Operaciones, que de igual forma se realizó para los demás.

Nota: Revisar imagen (*Fig.75. Almacenamiento de la llave pública creada en la consola desde el usuario Linux (Departamento de Operaciones) al servidor Ubuntu Server Keys*)

27.3. Encriptación y Almacenamiento de archivos en el repositorio SSH

Para este procedimiento se deben tener en cuenta varias etapas como lo son la creación y verificación del archivo de texto a encriptar ("prueba1.nano") en la ubicación de uno de los usuarios del Departamento de Operaciones, tal como se puede observar en la imagen (Fig.77).

Nota: Revisar imagen (*Fig.77. Verificación de la creación del archivo a encriptar en la consola del usuario Linux (Departamento de Operaciones)*)

Después se debe descargar la llave pública del usuario que desea ver la información real del archivo de texto (prueba1.nano), tal como se puede verificar en la imagen (Fig.79) del manual.

Nota: Revisar imagen (*Fig.79. Verificación de la descarga de la llave pública del usuario que requiere ver la información desde el servidor Ubuntu Server Keys al usuario Linux (Departamento de Operaciones)*)

Ahora ya teniendo la llave pública se procede a encriptar el archivo de texto (prueba1.nano) donde se verifica el archivo encriptado (prueba1.gpg) en su ubicación y el contenido después del proceso de encriptación, tal como se indica en las imágenes (Fig. 81) y (Fig. 82) del manual.

Nota: Revisar las imágenes (*Fig.81. y Fig.82. Proceso de verificación del archivo encriptado por el usuario Linux (Departamento de Operaciones*))

Por último se realiza el proceso de almacenamiento del archivo encriptado en el repositorio con seguridad Ubuntu Server SSH, tal como se muestra en la imagen de verificación (Fig.85) del proceso ingresando a la carpeta correspondiente al Departamento de Operaciones.

Nota: Revisar imágen (*Fig.85. Proceso de verificación de almacenamiento del archivo encriptado al repositorio Ubuntu Server SSH*)

27.4. Descarga y Des-Encriptación de archivos del repositorio Ubuntu Server SSH a los usuarios Linux (Departamento de Operaciones)

Teniendo en cuenta la información descrita anteriormente, ahora se debe descargar el archivo encriptado del repositorio con seguridad Ubuntu Server SSH a la ubicación que el usuario del Departamento de Operaciones que desea des-encriptar el archivo y obtener la información de importancia.

En la imagen (Fig.88) se puede verificar la ubicación del archivo descargado en la ubicación del usuario.

Nota: Revisar imagen (*Fig.88. Proceso de verificación de la descarga del archivo encriptado desde el repositorio Ubuntu Server SSH al usuario Linux (Departamento de Operaciones)*)

Ahora el proceso de des-encriptación del archivo de texto (“prueba1.gpg”) es muy sencillo ya que el usuario tiene la llave privada con la que se puede realizar este proceso según la definición de la criptografía o encriptación asimétrica.

Este resultado se puede observar en la imagen (Fig.90) donde se verifica la información real des-encriptada.

Nota: Revisar imagen (*Fig.90. Proceso de verificación del archivo des-encriptado mediante el uso de la llave privada del usuario Linux (Departamento de Operaciones))*

27.5. Creación de llaves pública y privada (Proceso de encriptación y des-encriptación de archivos para usuarios xp)

En los procesos anteriores se realizó la explicación de los resultados para los usuarios del Departamento de Operaciones con el sistema operativo Linux, ahora se explicarán los resultados obtenidos del proceso de creación de llaves públicas y privadas para los usuarios de los Departamentos de Ventas y Finanzas con el sistema operativo Xp.

Como se explicó en el capítulo anterior y en la sucesión de los pasos del manual, el resultado obtenido después de la creación de las llaves pública y privada gracias a la aplicación del software libre Kleopatra se puede visualizar en la imagen (Fig.110), donde se indican los ID que identifican cada una de las llaves.

Nota: Revisar imagen (*Fig.110. Proceso de generación de las llaves pública y privada en el programa Kleopatra para clientes Windows XP1 y XP2 (Departamentos de Ventas y Finanzas))*

27.6. Almacenamiento de llave pública desde el usuario al servidor Ubuntu Server Keys (para usuarios windows xp1 y xp2)

Este proceso es similar al realizado con el sistema operativo Linux sin embargo no se hace directamente en la consola del sistema operativo windows xp, se realiza con la ayuda del software libre Kleopatra.
Como se puede visualizar en la imagen (Fig.115) se debe ingresar la información descrita en el procedimiento para continuar con el almacenamiento de la llave pública del usuario del Departamento de Ventas (hleon) para el ejemplo del manual.

Nota: Revisar imagen (*Fig. 115. Proceso de almacenamiento de la llave pública desde el usuario (Departamentos de Ventas y Finanzas) al servidor Ubuntu Server Keys)*

27.7. Proceso de encriptación y almacenamiento de archivos en el repositorio Ubuntu Server SSH (para usuarios windows xp1 y xp2)

27.7.1. Proceso de Encriptación

Este proceso se realiza de manera diferente ya que solo basta con dar click derecho con el mouse sobre el archivo de imagen (Sunset.jpg) a encriptar, y se selecciona la opción de encriptación para empezar el procedimiento.

El resultado de la encriptación se puede observar en las imágenes (Fig.127 a Fig.129) donde se comprueba el funcionamiento del software libre Kleopatra.

Nota: Revisar las imágenes (*Fig. 127. A Fig.129. Proceso de encriptación de archivos mediante el uso de la llave pública del usuario Windows XP1 o XP2 que desea ver la información.)*

27.7.2. Proceso de almacenamiento de archivos en el repositorio Ubuntu Server SSH

Este procedimiento se realiza gracias a la ayuda de la aplicación PSFTP.exe, con la que se logra la conexión remota al repositorio con seguridad Ubuntu Server SSH con cualquiera de los usuarios de los Departamentos de Ventas o Finanzas.

El resultado de este proceso se puede verificar en la imagen (Fig.136), donde queda almacenado el archivo tipo imagen ("Sunset.jpg.gpg") en la carpeta de ventas.

Nota: Revisar las imágenes (*Fig.136. Proceso de almacenamiento de archivos desde el usuario Windows XP1 o XP2 al repositorio Ubuntu Server SSH)*

27.8. Proceso de descarga y des-encriptación de archivos del repositorio Ubuntu Server SSH a los usuarios Xp (Departamentos De Ventas Y Finanzas)

Como se explicó en el capítulo anterior este proceso de descarga y des-encriptación de archivos se realiza gracias a la ayuda de la aplicación PSFTP.exe, con la que se ingresa remotamente al repositorio con seguridad Ubuntu Server SSH con cualquier usuario de los Departamentos de Ventas o Finanzas, realizando el procedimiento descrito en el manual.

27.8.1. Proceso de descarga de archivos desde el repositorio Ubuntu Server SSH a los usuarios XP (Departamentos de Ventas y Finanzas)

Para la descarga de archivos se debe tener presente los comandos propios de la aplicación PSFTP.exe, donde se pueden visualizar con su información detallada mediante el ingreso del comando "help".

La verificación del archivo descargado del repositorio con seguridad se puede ver en las imágenes (Fig.142 y Fig.143) del manual de implementación.

Nota: Revisar las imágenes (*Fig.142 y Fig.143. Proceso de descarga de archivos desde el repositorio Ubuntu Server SSH al usuario Windows XP1 o XP2)*

27.8.2. Proceso de des-encriptación de archivos del repositorio Ubuntu Server SSH a los usuarios XP1 o XP2 (Departamentos de Ventas y Finanzas)

El proceso de des-encriptación del archivo descargado se realiza de manera similar a proceso de encriptación, tan solo basta con dar click derecho con el mouse sobre el archivo encriptado para iniciar el procedimiento descrito en la sucesión de los pasos del manual.

El resultado de este proceso se puede observar en las imágenes (Fig.148 y Fig.149) del manual.

Nota: Revisar las imagenes (*Fig.148 y Fig.149. Proceso de des-encriptación de archivos en el equipo del usuario Windows XP1 o XP2 (Departamentos de Ventas y Finanzas))*

27.9. Enjaulado de usuarios en el repositorio Ubuntu Server SSH

El proceso de enjaulado de usuarios de la empresa es importante ya que garantiza la privacidad y exclusividad de los usuarios de la empresa al momento de ingresar al repositorio con seguridad, debido a que los usuarios ingresarán únicamente a la carpeta correspondiente a su departamento y no podrá ingresar a las otras.

Como se puede visualizar en la imagen (Fig.155 a Fig.158), se puede verificar el funcionamiento del procedimiento realizado.

Nota: Revisar imagen (*Fig.155 a Fig.158. Proceso de enjaulado de usuarios en el repositorio Ubuntu Server SSH)*

27.10. Instalación de Firewall (IP-Tables)

Como último proceso a tener en cuenta, es importante en la implementación del repositorio con seguridad la instalación del firewall (IPTABLES), ya que garantiza la seguridad de la información de los usuarios de los diferentes departamentos de la empresa en cuanto a la transferencia de archivos, mediante la asignación de reglas permitiendo el filtrado del tráfico de red.

En este caso las reglas o parámetros de funcionamiento del firewall aplicadas al repositorio con seguridad, se pueden visualizar en la imagen (Fig.160) del manual.

Nota: Revisar imagen (*Fig.160. Proceso de Instalación de Firewall en el repositorio Ubuntu Server SSH)*

Tal como se propuso en los objetivos del proyecto, se han cumplido con las metas y alcances del proyecto, donde se puede verificar el óptimo funcionamiento de cada uno de los procesos desarrollados a lo largo del manual de implementación del repositorio con seguridad.

A nivel social, la implementación del proyecto ayuda a la mejor organización y seguridad de la información de la empresa brindando la privacidad, exclusividad y seguridad que tanto necesita la empresa para el manejo de sus archivos.

Capítulo V

Conclusiones

A lo largo del documento se logró observar que el proyecto se dividió en diferentes etapas las cuales, van entrelazadas la una con la otra, es decir, que cada una depende la anterior tal y como se visualizó en el manual de implementación del repositorio con seguridad.

De acuerdo con lo anterior, se puede concluir que el proceso de generación de llaves pública y privada fue más sencillo, organizado, completo y rápido de desarrollar en el sistema operativo Windows Xp gracias al software libre Kleopatra, que en comparación con el sistema operativo Linux (método trabajado por la consola "terminal" en Linux - (Generación de las llaves por consola)) era más lento, ya que solicitaba al usuario realizar tareas alternas para generar más entropía y así obtener más bytes aleatorios para la creación de las llaves pública y privada de 2048 bits. Sin embargo, el método utilizado, gracias a la aplicación del sistema operativo Linux "Contraseñas y claves" (Modo gráfico de generación de llaves), se logró generar las llaves públicas y privadas de manera similar al software libre Kleopatra con la misma facilidad, orden y rapidez.
Por otro lado, la generación de entropía en el sistema operativo Linux brindo mayor seguridad a las llaves públicas que las creadas en el sistema operativo Windows, evitando posibles casos de sabotaje al proceso de seguridad.

Debido al proceso de creación, fue necesaria la instalación del paquete SKS-KEYSERVER (OPEN PGP) en el servidor de llaves Ubuntu Server Keys, ya que permitió el almacenamiento efectivo de llaves públicas para el proceso de encriptación de archivos de los diferentes usuarios de la empresa sin importar el sistema operativo desde donde se haga.

Por consiguiente, el proceso de encriptación de archivos fue exitoso, debido a que se obtuvieron resultados similares en cuanto a procedimiento y desarrollo del mismo en cada sistema operativo. Sin embargo, se generaron algunas diferencias en los tiempos de encriptación. Es por esto, que dependiendo del tipo de archivo al cual se requiere realizar el proceso de encriptación y el sistema operativo en el que se realice, los tiempos variarán como se observó en la tabla de tiempos de encriptación, donde en el sistema operativo Windows se realizaron de manera más rápida, sin importar el tipo de archivo; mientras que en el sistema operativo Linux, los tiempos aumentaron considerablemente dependiendo del tamaño y tipo de archivo al que se le realizo el proceso como por ejemplo los archivos tipo imagen que tomaron más tiempo que los de tipo texto, todo debido al proceso interno que tiene que realizar el ordenador físico y el sistema operativo para encriptar el archivo.

Por lo anterior, el almacenamiento de archivos se realizó de manera correcta, ya que se pudo verificar cada archivo encriptado en las carpetas correspondientes de cada usuario en el repositorio con seguridad Ubuntu Server SSH, tal como lo indicó el manual de implementación del repositorio con seguridad.

Como consecuencia del proceso de almacenamiento de archivos, la des-encriptación de archivos fue exitosa, teniendo en cuenta que se tuvieron resultados similares en cuanto al procedimiento y desarrollo del mismo en cada sistema operativo. Sin embargo, se presentaron diferencias entre los tiempos de ejecución del proceso teniendo en cuenta que en el sistema operativo Windows se obtuvieron tiempos iguales en los dos tipos de archivo (tipo imagen (.jpg) y tipo texto (.txt)) similares a los de encriptación, debido a que el programa Kleopatra maneja menos tiempos de procesamiento de tareas (creación de llaves, encriptación y des-encriptación) y no necesita la generación de bytes aleatorios para la creación de llaves. En el caso del sistema operativo Linux, los tiempos de des-encriptación aumentaron al doble en ambos tipos de archivos debido a que este sistema operativo requiere de la generación de entropía (Generación de bits aleatorios recogidos por un sistema operativo o aplicación para el uso de criptografía u otros programas que requieren de datos aleatorios. Esta generación de datos aleatorios se obtiene por lo general con fuentes de hardware tales como movimientos con el mouse, apertura y trabajo en programas del sistema operativo, etc)) la cual hace que las llaves públicas y privadas sean más seguras; sin embargo, en el caso del archivo tipo imagen aumento un poco más, ya que este tiene mayor tamaño que el archivo tipo texto.

Como conclusión principal y partiendo de lo anterior, en ambos sistemas operativos fue exitoso el desarrollo de los procesos de encriptación y des-encriptación, ya que mediante el uso de las herramientas utilizadas, tanto en consola como en los software libres, permitió la verificación de cada uno de los procedimientos de forma detallada, versátil e interactivo para los usuarios de la empresa; todo esto gracias a la previa investigación del concepto de encriptación asimétrica.

Por otra parte, el último proceso de implementación del repositorio con seguridad fue el proceso de enjaulado de usuarios, ya que permitió que cada uno de los usuarios de la empresa, al momento de ingresar al repositorio con seguridad de forma remota, únicamente pudieran ingresar a los archivos y a la carpeta propia del departamento al que pertenezca. Este proceso, como se pudo verificar en el manual de implementación y en el capítulo relacionado con los resultados del proyecto, es fundamental para la implementación del repositorio con seguridad, ya que garantiza la privacidad y exclusividad de las carpetas entre los departamentos de la empresa, ofreciendo mayor seguridad al proceso de transmisión de archivos, ya que si un usuario externo a la empresa desea acceder a la información de cierta carpeta, no podrá hacerlo, ya que no tiene la contraseña de cada usuario de la empresa ni tampoco tiene la información de la llave privada para des-encriptar la información del repositorio.

Hasta el momento se han descrito los procesos de mayor impacto en el proyecto. Sin embargo, falta aclarar un detalle importante como lo es la seguridad en el medio de transmisión de la información del repositorio. Partiendo de lo anterior, la instalación del firewall (IPTABLES) fue necesaria, ya que para el proyecto es un valor agregado el garantizar la seguridad de la información de los usuarios de los diferentes departamentos de la empresa, en cuanto a la transferencia de archivos mediante la asignación de reglas, permitiendo el filtrado del tráfico de red. En otras palabras, el

firewall es un blindaje para el medio de transmisión de la información evitando el sabotaje de agentes externos indeseados en la empresa.

Por otro lado el protocolo SSH fue de gran ayuda ya que a diferencia de otros protocolos como el Telnet, ofreció un servicio en ambos sistemas operativos de fácil manejo, entendible, confiable y lo más importante seguro para la transmisión de datos entre los Departamentos de la empresa y el repositorio con seguridad Ubuntu Server SSH.
Hablando del sistema de seguridad RSA se logró visualizar que fue una herramienta útil y de fácil manejo para el intercambio de claves de forma segura entre los usuarios de los Departamentos de la empresa y el servidor de llaves públicas Ubuntu Server Keys, que a diferencia de sistemas como el DES que es muchísimo más rápido pero inseguro dependiendo del tipo de aplicación que se maneje.

Cabe aclarar que para el manejo eficiente del proyecto, se requiere de cierto nivel de manipulación informática, es decir, que los usuarios de la empresa necesitan de una previa capacitación en la que se les explique de manera concreta el proceso de encriptación asimétrica incluyendo la generación de llaves pública y privada.

A manera de sugerencia para la implementación adecuada del proyecto, se requiere hacer la inversión monetaria a un computador o máquina física en la que se disponga de las características físicas mínimas mencionadas a lo largo del proyecto para su correcto funcionamiento.

Todo lo mencionado en la parte preliminar de este capítulo, está relacionado con el desarrollo del proyecto a nivel técnico; sin embargo es de vital importancia dar a conocer los aportes en el ámbito social.

Mediante la implementación de este proyecto se logró dar solución al inconveniente que tenía la empresa relacionada con la seguridad de archivos, ofreciendo un repositorio con seguridad a bajo costo donde se utilizaron software libres que permitieron su implementación; garantizando las características de confidencialidad, integridad, disponibilidad, utilidad, organización y fácil manejo de la información los cuales generaron mayor eficiencia en los procesos internos de la empresa. Este tipo de proyecto se puede implementar en cualquier empresa que tenga diferentes sucursales en el manejo de ficheros (carpetas) para su mayor organización garantizando el correcto manejo de las herramientas y brindando mejores resultados en los procesos internos.

Finalmente en el campo personal y profesional, la implementación de este proyecto aportó en los conocimientos en el área de telecomunicaciones y sistemas, como valor agregado a los ya adquiridos en el transcurso de la formación profesional en el campo de la ingeniería electrónica; los cuales ayudaron en la experiencia laboral adquirida a lo largo de la práctica y del trabajo actual desempeñado en la empresa.

BIBLIOGRAFIA

[1] Repositorio digital: http://bibliotecabiologia.usal.es/tutoriales/catalogos-repositorios-bibliosvirtuales/repositorios_digitales.html

[2] Encriptación: http://www.informatica-hoy.com.ar/seguridad-informatica/Criptografia.php

[3] Criptografía asimétrica: https://www.cert.fnmt.es/curso-de-criptografia/criptografia-de-clave-asimetrica

[4] Criptografía simétrica: https://www.cert.fnmt.es/curso-de-criptografia/criptografia-de-clave-simetrica

[5] Protocolo SSH: http://www.gb.nrao.edu/pubcomputing/redhatELWS4/RH-DOCS/rhel-rg-es-4/ch-ssh.html, http://katherynnparedes.blogspot.com.br/2013/04/tipos-de-protocolo.html, https://wiki.archlinux.org/index.php/Secure_Shell_(Espa%C3%B1ol), http://www.redeszone.net/gnu-linux/servidor-ssh-en-ubuntu/, http://ocw.uoc.edu/computer-science-technology-and-multimedia/advanced-aspects-of-network-security/advanced-aspects-of-network-security/P06_M2107_01772.pdf, http://www.gb.nrao.edu/pubcomputing/redhatELWS4/RH-DOCS/rhel-rg-es-4/s1-ssh-conn.html, http://www.gb.nrao.edu/pubcomputing/redhatELWS4/RH-DOCS/rhel-rg-es-4/s1-ssh-conn.html, http://www.gb.nrao.edu/pubcomputing/redhatELWS4/RH-DOCS/rhel-rg-es-4/s1-ssh-conn.html, http://web.mit.edu/rhel-doc/3/rhel-rg-es-3/s1-ssh-version.html https://wiki.archlinux.org/index.php/Secure_Shell_(Espa%C3%B1ol)

[6] Sistema de seguridad RSA: https://www.uam.es/personal_pdi/ciencias/ehernan/Talento/Maria%20Jesus%20Vazquez/criptorsa.pdf, https://seguinfo.wordpress.com/2007/09/14/%C2%BFque-es-rsa/, https://www.youtube.com/watch?v=9ReP4lmExmc, http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/rsa.html, http://serdis.dis.ulpgc.es/~ii-cript/RSA.pdf, https://opardoiphone.wordpress.com/2013/05/01/ejercicio-11-teorema-chino-del-resto/

[7] Segmentación de redes: http://ipv4to6.blogspot.com.br/p/segmentacion.html

[8] Protocolo TCP/ip v4: http://ipv4to6.blogspot.com.br/p/protocolo-ipv4.html

[9] Protocolo TCP/ip v6: http://www.ipv6.es/es-ES/introduccion/Paginas/QueesIPv6.aspx

[10] Firewall e IPtables: http://www.pello.info/filez/firewall/iptables.html, http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/cortafuegos_iptables.html)

[11] HERNANDEZ PEREZ, Tony; RODRIGUEZ MATEOS, David y BUENO DE LA FUENTE, Gema. Open Access: el papel de las bibliotecas en los repositorios institucionales de acceso abierto. The role of libraries in open access institutional repositories. Vol. 10. Murcia: Murcia, Universidad de Murcia, Servicio de Publicaciones, 2007. 188p. ISS 1575-2437.

[12] OVIEDO, Nestor; LIRA, Ariel; Martinez, Santiago y PINTO, Analia. SeDiCI - Desafíos y experiencias en la vida de un repositorio digital. e-colabora; vol. 1, no. 2. La Plata, Argentina: 2011. 4p.

[13] BARTON, Mary y WATERS, Margaret. Como crear un repositorio institucional. Cambridge: The Cambridge-MIT Institute (CMI), 2004-2005. 16p.

[14] PARADELO, Aída. Preservación Documental en Repositorios Institucionales. Vol 23. Mexico: INVESTIGACIÓN BIBLIOTECOLOGICA, 2008-2009. 244p.

[15] ESPAÑA, ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN ISO. ISO 23081-1 (Abril-Junio, 2006). Información y documentación - Procesos de gestión de documentos - Metadatos para la gestión de documentos. Parte 1. Madrid. 2006. ISSN 0210-0614. p. 1-29.

[16] GIRALT, Olga; VIDAL, Carmen; PEREZ, Carlos. Seguridad de los Documentos de Archivo: Estudio de Caso del archivo del ayuntamiento de Barcelona. Vol 20. Barcelona, España: El Profesional de la Información, 2011. 2p. ISSN 1386-6710.

[17] TÉRMENS, Miguel. Investigación y desarrollo en preservación digital: un balance internacional. Vol 18. España: El Profesional de la Información, 2009. 11p. ISSN 1386-6710.

[18] ADAME, Silvia; LLORÉNZ, Luis. Retrospectiva de los repositorios de acceso abierto y tendencias en la socialización del conocimiento. Vol 15. México: Revista Electrónica de Investigación Educativa, 2013. 16p. ISSN 1607-4041.

[19] GÓMEZ, Oiner; BAUTA, René; ESTRADA, Vivian. Modelo para la compartimentación de la información en las organizaciones. Vol 45. Cuba: Ciencias de la Información, 2014. 7p. ISSN 0864-4659.

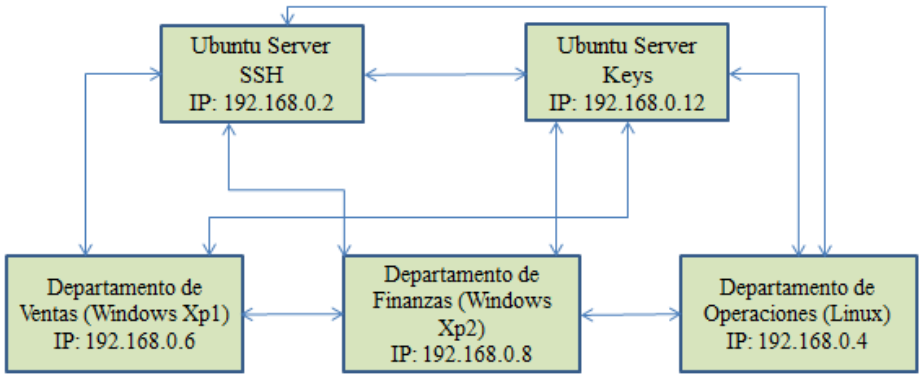
[20] Información de Virtual Box: http://virtualbox.es/caracteristicas/

[21] Información de Kleopatra: http://www.ecured.cu/index.php/Kleopatra

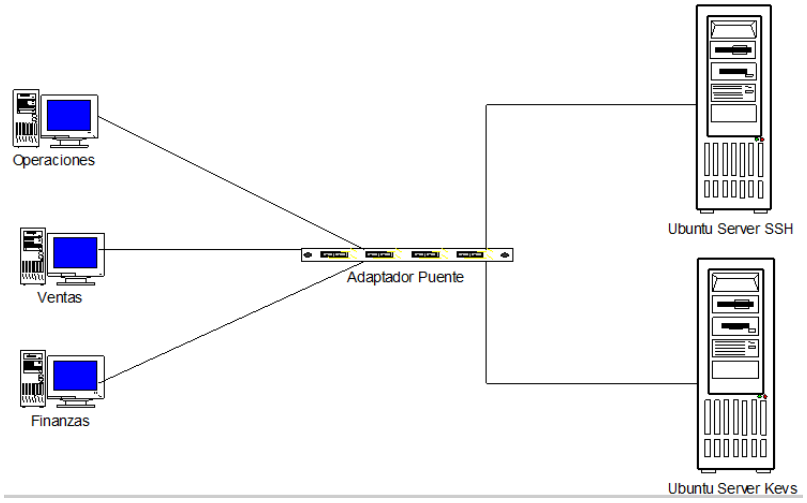
ANEXOS

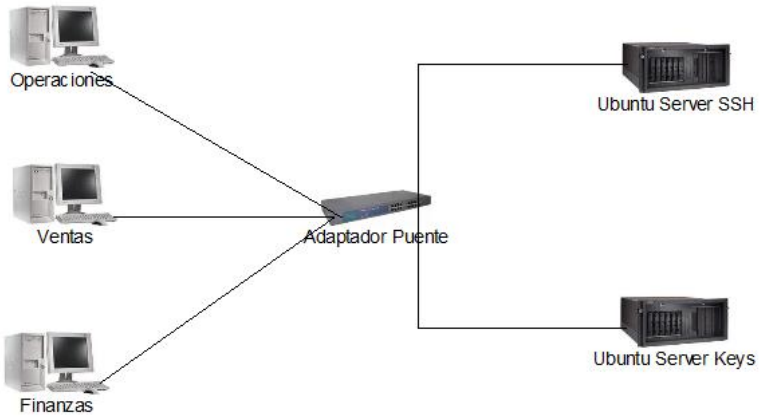
A.1 Diagrama de comunicación entre máquinas virtuales

Siguiendo la estructura del siguiente diagrama se realizará la comunicación entre máquinas virtuales mediante el comando Ping:

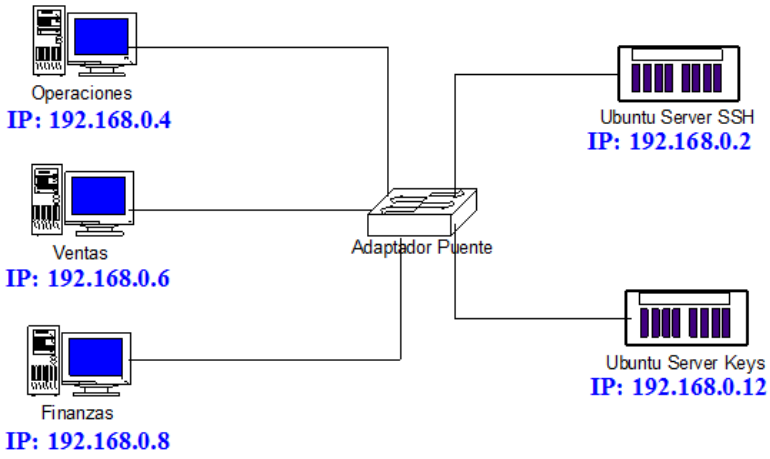


A.2 Topología de Red del sistema (representación con equipos físicos)





A.3 Topología de Red del sistema (representación con simbología de red)



A.4 Manual de implementación del repositorio con seguridad

Contenido

- Instalación del software virtualizador VIRTUAL BOX.
- Montaje de máquinas virtuales (Windows XP, Linux, Ubuntu Server SSH o Ubuntu Server Keys).
- Instalación del paquete OPENSSH en Ubuntu Server SSH
- Prueba de comunicación entre máquinas virtuales con el servidor.
- Creación de usuarios, grupos y carpetas en el servidor.
- Prueba de conexión remota al servidor con los usuarios creados.
- Instalación del paquete SKS-KEYSERVER (OPENPGP) en Ubuntu Server Keys.
- Creación de llaves pública y privada (para el proceso de encriptación y des-encriptación de archivos)

- Creación de llaves pública y privada con GNUPG.
- Almacenamiento de llaves públicas desde el usuario al servidor Ubuntu Server Keys.
- Encriptación y almacenamiento de archivos en el repositorio Ubuntu Server SSH.
- Descarga y des-encriptación de archivos del repositorio Ubuntu Server SSH a los usuarios Linux (Departamento de Operaciones).
- Instalación de la aplicación GPG4WIN (Software libre Kleopatra)
- Creación de llaves pública y privada (para el proceso de encriptación y des-encriptación de archivos para usuarios XP) con el Software Kleopatra.
- Almacenamiento de llave pública desde el usuario al Servidor Ubuntu Server Keys (para usuarios Windows xp1 y xp2)
- Proceso de encriptación de archivos y almacenamiento de archivos en el repositorio Ubuntu Server SSH (Para usuarios XP)
- Proceso de descarga y des-encriptación de archivos del repositorio Ubuntu Server SSH a los usuarios XP (Departamento de Ventas y Finanzas).
- Enjaulado de Usuarios.
- Instalación de IPTABLES (FIREWALL).

INSTALACION DEL SOFTWARE VIRTUALIZADOR VIRTUALBOX:

Para la implementación del repositorio con seguridad se necesita la instalación del software libre de virtualización VirtualBox.

1. Primero se debe abrir el archivo ejecutable del programa, donde se abrirá una ventana emergente en la que se dará click en el icono “next” para empezar la instalación.

Fig.7. Proceso de instalación software virtualizador VIRTUALBOX

2. Ahora se abrirá otra ventana en la que pedirá al usuario seleccionar la ubicación de la instalación del software virtualizador. Luego se da click en el icono “next” para continuar la instalación.

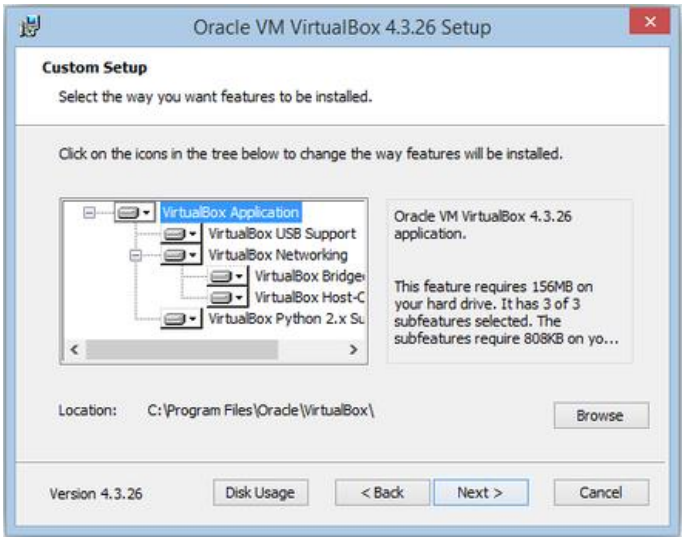


Fig.8. Proceso de instalación software virtualizador VIRTUALBOX

3. Después aparecerá otra ventana en la que se seleccionarán opciones de accesos directos y extensiones del software. Se da click en el icono “next” para continuar con el proceso.

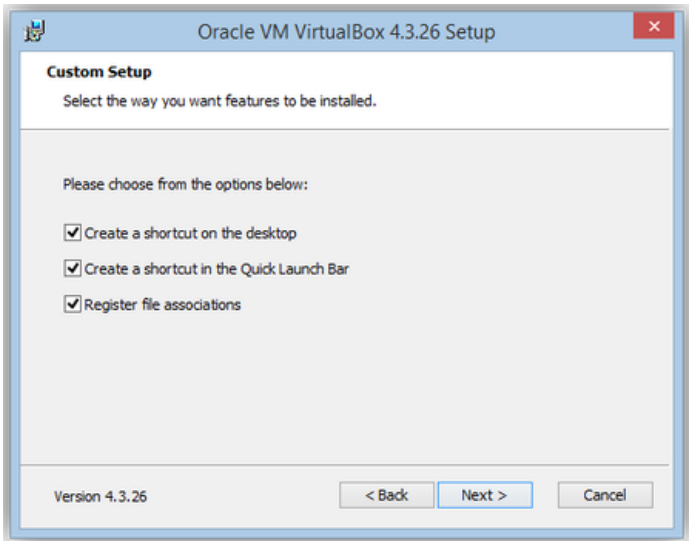


Fig.9. Proceso de instalación software virtualizador VIRTUALBOX

4. Luego el programa generará una ventana emergente en la que advertirá al usuario que se van a copiar los archivos, se reiniciarán las tarjetas de red y se instalará el programa. Se da click en el icono “install” para continuar.

Fig.10. Proceso de instalación software virtualizador VIRTUALBOX

Se abrirá una ventana en la que le indicará al usuario el proceso de instalación del software virtualizador.

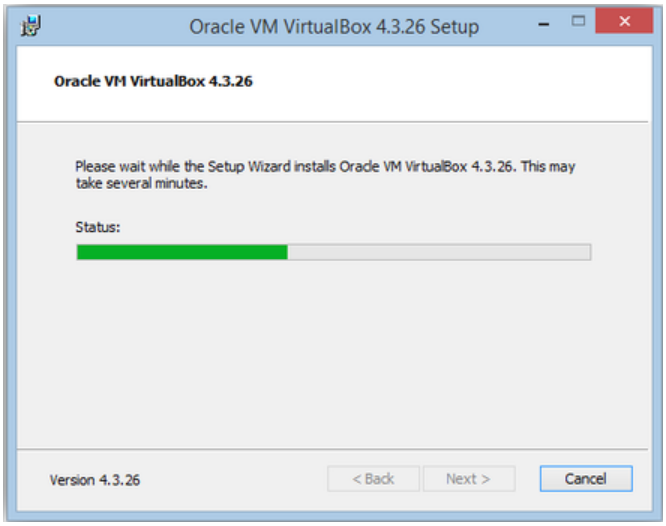


Fig.11. Proceso de instalación software virtualizador VIRTUALBOX

5. Por último, se generará una ventana en la que le indicará al usuario que el programa ha sido instalado correctamente. Se da click en el icono “Finish” para terminar.

Fig.12. Proceso de instalación software virtualizador VIRTUALBOX

MONTAJE DE MÁQUINAS VIRTUALES (WINDOWS XP, LINUX, UBUNTU SERVER SSH Y UBUNTU SERVER KEYS)

El siguiente paso fundamental es instalar (montar) las máquinas virtuales en las que se implementará todo el desarrollo del repositorio con seguridad.
Cabe aclarar que cada una de las máquinas virtuales se instala de igual manera sin importar el sistema operativo, lo único que cambia es la manera en la que se va a asignar el espacio de almacenamiento y memoria RAM.

1. Una vez se da click en el acceso directo "Oracle VM Virtual Box", se abrirá una ventana emergente en la que se debe dar click en el icono "Nueva", que se encuentra en la parte superior izquierda.

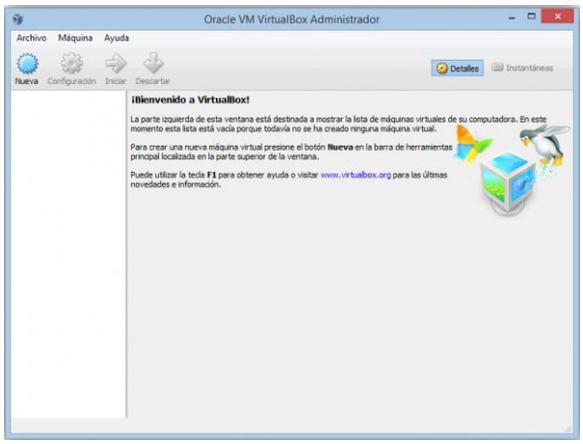


Fig.13. Proceso de montaje de máquinas virtuales (Windows xp, Linux, Ubuntu Server SSH o Ubuntu Server Keys)

2. A continuación se abrirá una ventana emergente en la que pedirá el nombre de la máquina virtual, el tipo de sistema operativo y la versión del mismo (Para el caso del proyecto se toma el mismo procedimiento para los diferentes sistemas operativos a implementar).

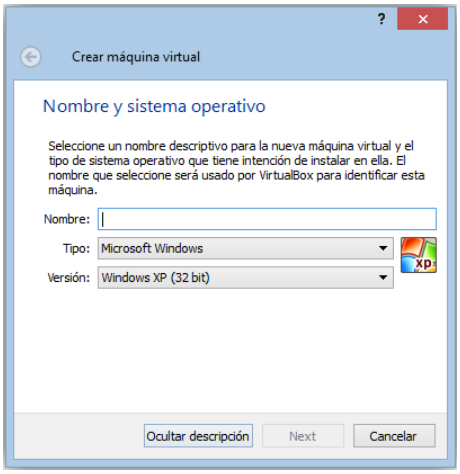


Fig.14. Proceso de montaje de máquinas virtuales (Windows xp, Linux, Ubuntu Server SSH o Ubuntu Server Keys)

3. Ahora se deberá seleccionar la cantidad de momoria RAM del sistema operativo (cambia de acuerdo al sistema operativo que se desee montar).

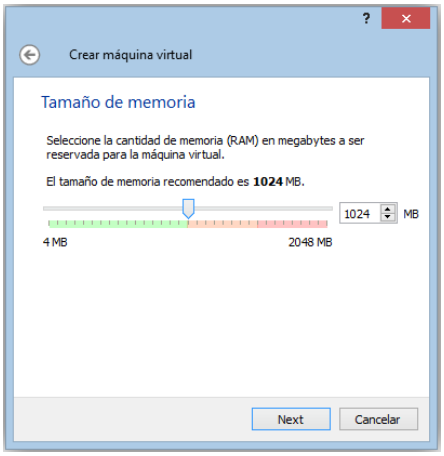


Fig.15. Proceso de montaje de máquinas virtuales (Windows xp, Linux, Ubuntu Server SSH o Ubuntu Server Keys)

4. Después se debe seleccionar la opción “Crear un disco duro virtual”, para continuar con el proceso.

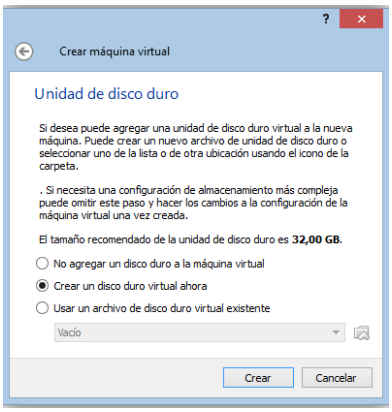


Fig.16. Proceso de montaje de máquinas virtuales (Windows xp, Linux, Ubuntu Server SSH o Ubuntu Server Keys)

5. Teniendo la configuración básica de la máquina virtual, se genera una ventana donde resumirá la información ingresada para el montaje de la maquina virtual.

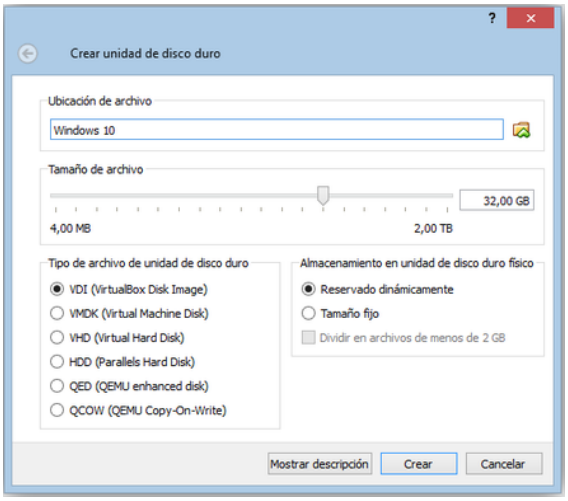


Fig.17. Proceso de montaje de máquinas virtuales (Windows xp, Linux, Ubuntu Server SSH o Ubuntu Server Keys)

6. Por último, queda inicializar la máquina virtual para proceder con la implementación del repositorio con seguridad.

Fig.18. Proceso de montaje de máquinas virtuales (Windows xp, Linux, Ubuntu Server SSH o Ubuntu Server Keys)

INSTALACION DEL PAQUETE OPENSSH EN UBUNTU SERVER SSH

Teniendo instalada la máquina virtual correspondiente al repositorio Ubuntu Server SSH, es necesario instalar el paquete OpenSSH que va a permitir la conexión segura de los usuarios para la carga y descarga de archivos.

1. Primero se instala el paquete OpenSSH mediante el siguiente comando:

   Sudo apt-get install openssh-server

2. Ahora se debe realizar la configuración del servidor SSH mediante el siguiente comando:

   Sudo gedit /etc/ssh/sshd_config

3. A continuación se configura el puerto por el cuál se va a comunicar SSH, por defecto es el 22. Se debe abrir un puerto en el cual re-direccione la IP interna de la máquina virtual donde lo tengamos.

   #Package generated configuration file
   # See the sshd_config(5) manpage for details
   PORT 1234

4. Después se asigna el protocolo 2 de SSH para que siempre conecte mediante el, ya que es mucho más seguro para las conexiones de los usuarios.

   Protocol 2

5. Luego se asigna la ubicación en la que se almacenaran las llaves RSA generadas.

   #HostKeys for protocol versión 2
   HostKeys /etc/ssh/ssh_host_rsa_key
   HostKey /etc/ssh/ssh_host_dsa_key
   #Privilege Separation is turne don for security

UsePrivilegeSeparation yes
KeyRegenerationInterval 3600
ServerKeyBits 2048

6. Ahora se asignan permisos para autorizar el Loggin.

SyslogFacility AUTH
LogLevel INFO

7. Luego se deben agregar permisos de autenticación (Permit Root Loggin).

LoginGraceTime 120
PermitRootLogin no
StrictModes yes

8. Después se agrega la autenticación RSA para la publicación de llaves y su ubicación en el servidor Ubuntu Server Keys.

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

9. A continuación no se debe habilitar la opción de cambiar las contraseñas (passwords)

PermitEmptyPasswords no

10. Por último se ajustan configuraciones de ventana.

X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes

PRUEBA DE COMUNICACIÓN ENTRE MÁQUINAS VIRTUALES CON LOS SERVIDORES

Teniendo montadas todas las máquinas virtuales de cada uno de los sistemas operativos incluyendo los servidores, ahora se asignan direcciones IP fijas a cada máquina virtual para permitir la comunicación entre ellas y así empezar a implementar el repositorio con seguridad.
Los sistemas operativos se identifican de la siguiente manera:

Windows XP1:

Representa al departamento de Ventas y tiene la dirección IP: 192.168.0.6

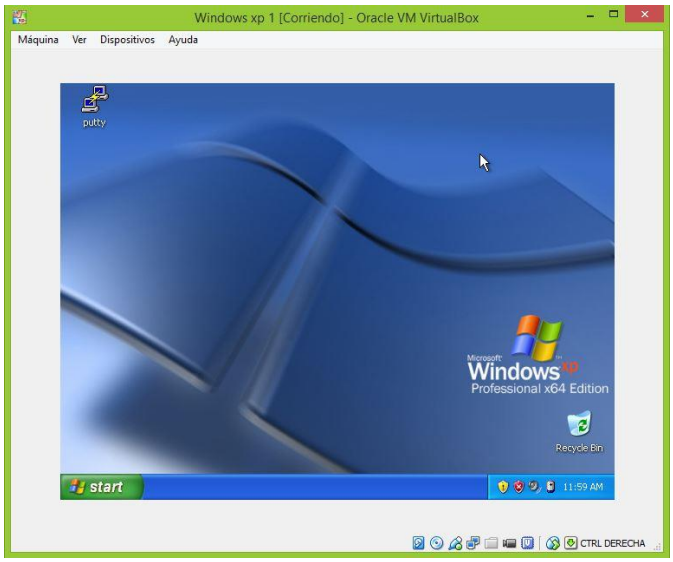


Fig.19. Windows XP1 (Representa al departamento de Ventas)

Windows XP2:

Representa al departamento de Finanzas y tiene la dirección IP: 192.168.0.8

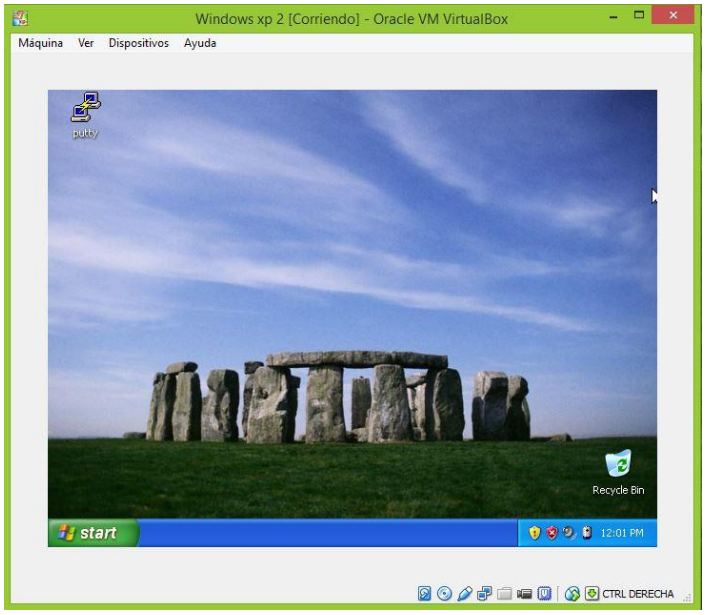


Fig.20. Windows XP2 (Representa al departamento de Finanzas)

Linux:

Representa al departamento de Operaciones y tiene la dirección IP: 192.168.0.4

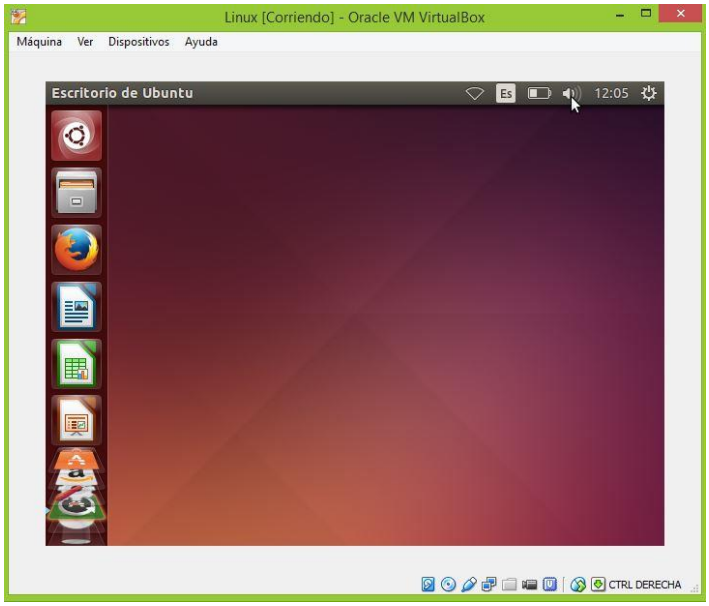


Fig.21. Linux (Representa al departamento de Operaciones)

Ubuntu Server SSH (servidor):

Representa el repositorio con seguridad el cual tiene la dirección IP: 192.168.0.2

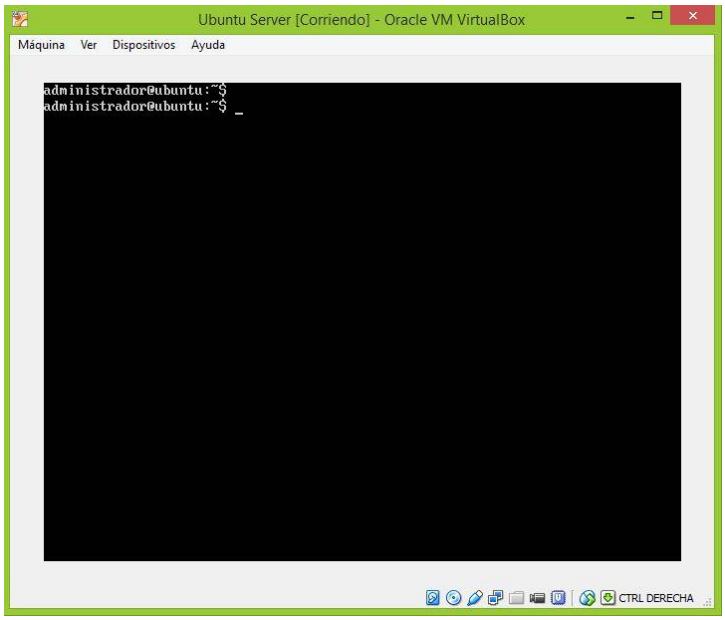


Fig.22. Ubuntu Server SSH (Representa el repositorio con seguridad)

Ubuntu Server Keys (servidor):

Representa el servidor de llaves públicas de los usuarios de la empresa el cual tiene la dirección IP: 192.168.0.12

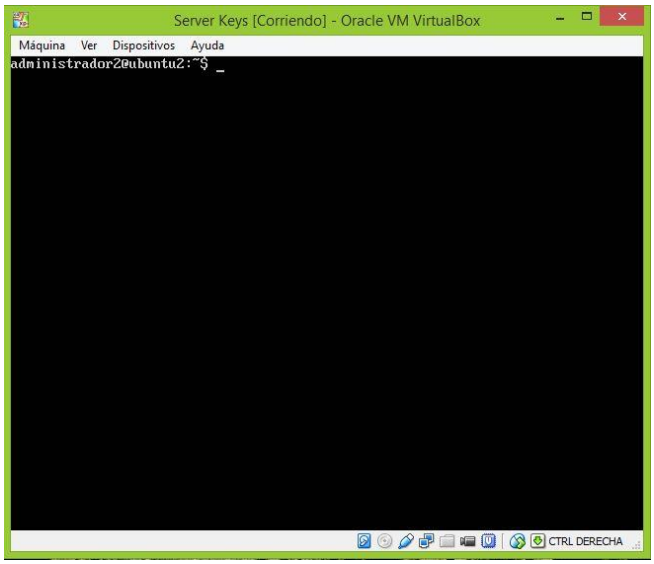


Fig.23. Ubuntu Server Keys (Representa el servidor de llaves públicas de los usuarios de la empresa)

Teniendo identificadas las máquinas virtuales con sus respectivas direcciones IP, ahora se realiza la comunicación entre ellas de acuerdo a la siguiente imagen:

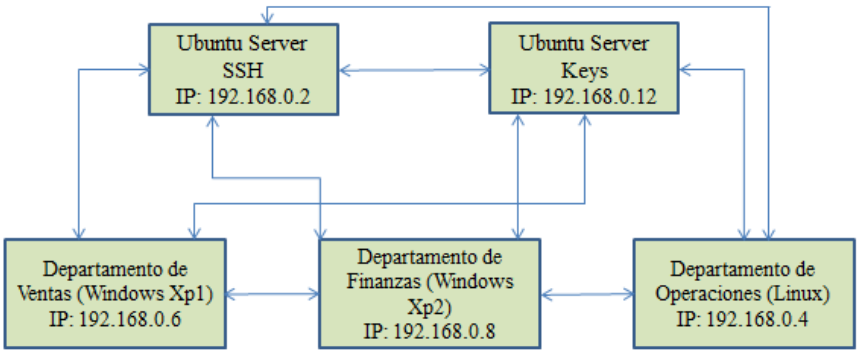


Fig.24. Diagrama de comunicación entre máquinas virtuales

Comunicación entre Ubuntu Server SSH (servidor) - Windows XP1 (cliente):

- Desde Ubuntu Server SSH (servidor) a XP1.

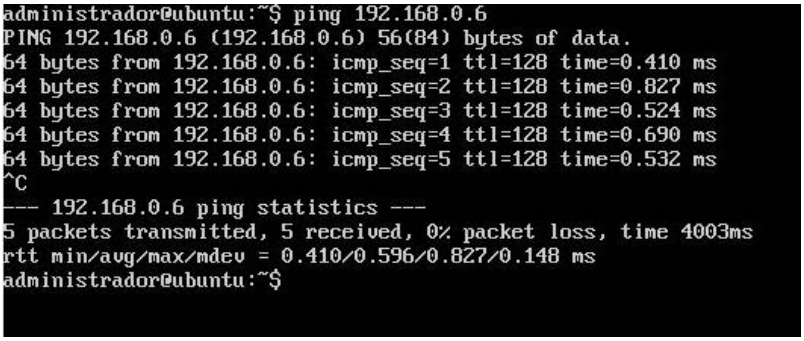


Fig.25. Comunicación de máquinas virtuales desde Ubuntu Server SSH (servidor) a XP1

- Desde XP1 a UBUNTU SSH Server.

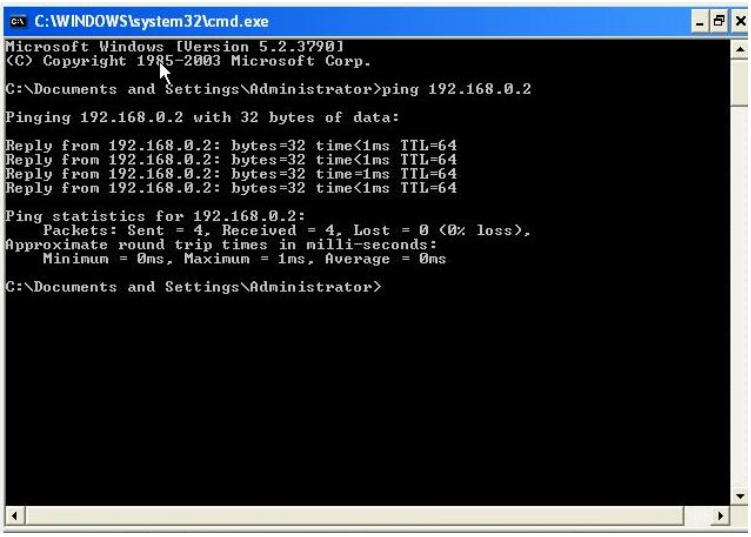


Fig.26. Comunicación de máquinas virtuales desde XP1 a Ubuntu Server SSH

Comunicación entre Ubuntu Server SSH (servidor) - Windows XP2:

- Desde Ubuntu Server SSH (servidor) a XP 2.

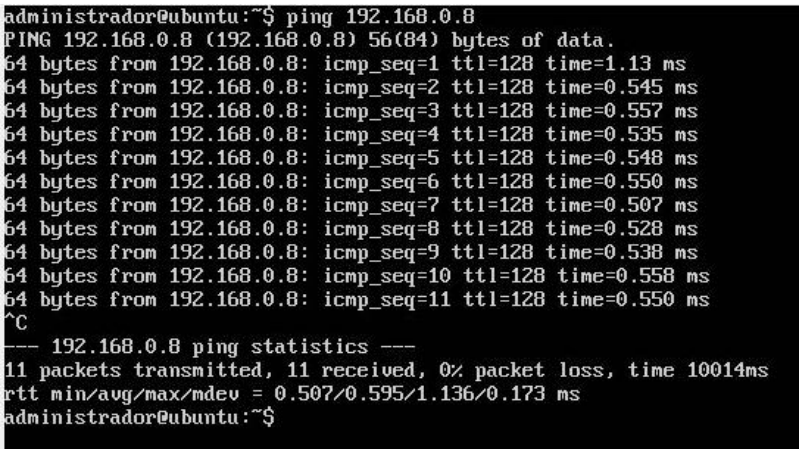


Fig.27. Comunicación de máquinas virtuales desde Ubuntu Server SSH (servidor) a XP2

- Desde XP2 a Ubuntu Server SSH (servidor).

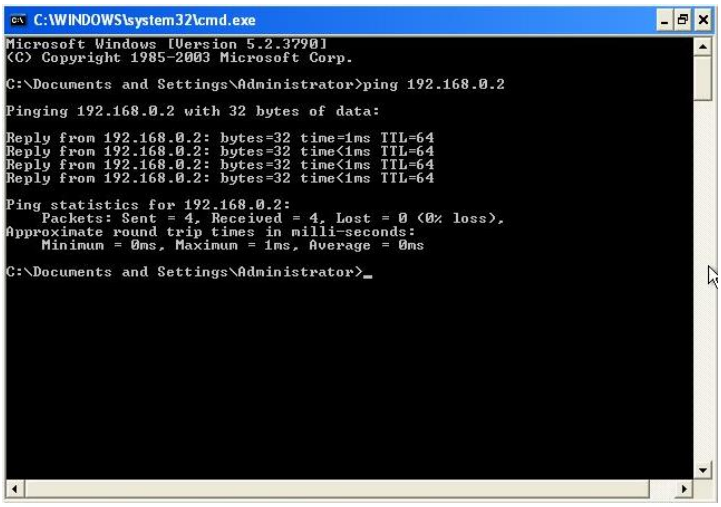


Fig.28. Comunicación de máquinas virtuales desde XP2 a Ubuntu Server SSH (servidor)

Comunicación entre Ubuntu Server SSH (servidor) - Linux:

- Desde Ubuntu Server SSH (servidor) a Linux.

Fig.29. Comunicación de máquinas virtuales desde Ubuntu Server SSH a Linux.

- Desde Linux a Ubuntu Server SSH (servidor)

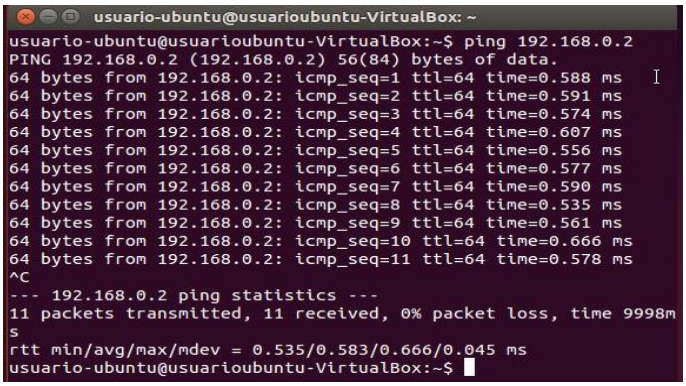


Fig.30. Comunicación de máquinas virtuales desde Linux a Ubuntu Server SSH (servidor)

Comunicación entre Ubuntu Server Keys (servidor) - Windows XP1:

- Desde Ubuntu Server Keys (servidor) a XP1 y desde XP1 a Ubuntu Server Keys.

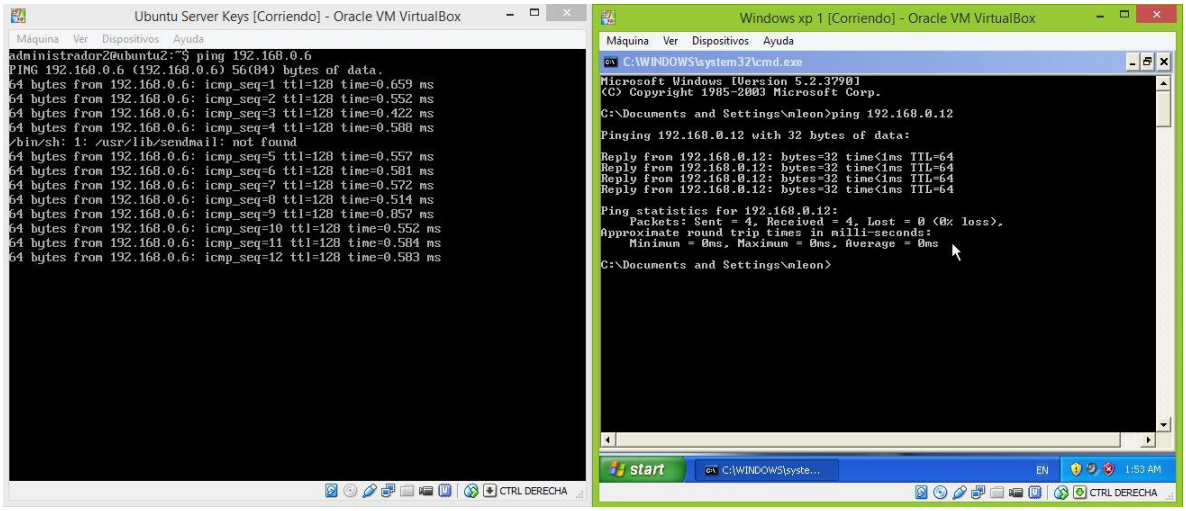


Fig.31. Comunicación de máquinas virtuales desde Ubuntu Server Keys (servidor) a XP1 y desde XP1 a Ubuntu Server Keys

Comunicación entre Ubuntu Server Keys (servidor) - Windows XP2:

- Desde Ubuntu Server Keys (servidor) a XP2 y desde XP2 a Ubuntu Server Keys (servidor).

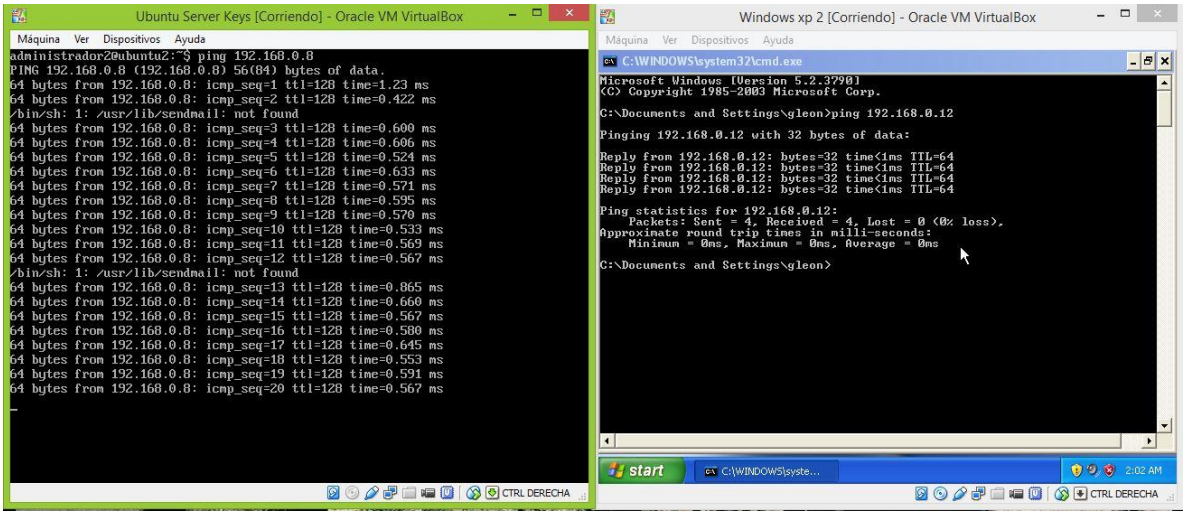


Fig.32. Comunicación de máquinas virtuales desde Ubuntu Server Keys (servidor) a XP2 y desde XP2 a Ubuntu Server Keys (servidor)

Comunicación entre Ubuntu Server Keys (servidor) - Linux:

- Desde Ubuntu Server Keys (servidor) a Linux y desde Linux a Ubuntu Server Keys (servidor).

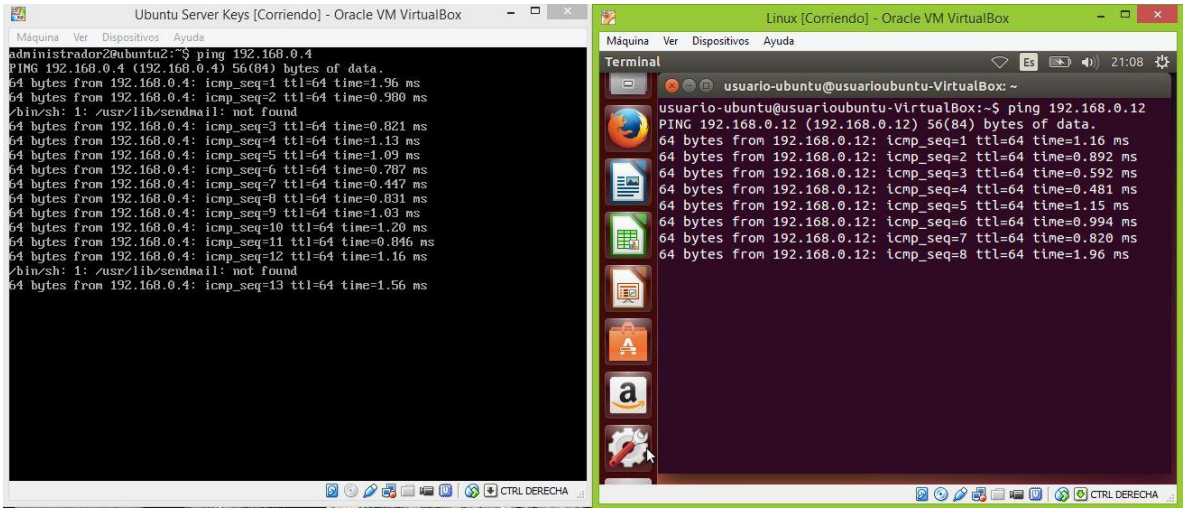


Fig.33. Comunicación de máquinas virtuales desde Ubuntu Server Keys (servidor) a Linux y desde Linux a Ubuntu Server Keys (servidor)

Comunicación entre Ubuntu Server Keys (servidor) - Ubuntu Server SSH (servidor):

- Desde Ubuntu Server Keys (servidor) a Ubuntu Server SSH (servidor) y desde Ubuntu Server SSH (servidor) a Ubuntu Server Keys (servidor).

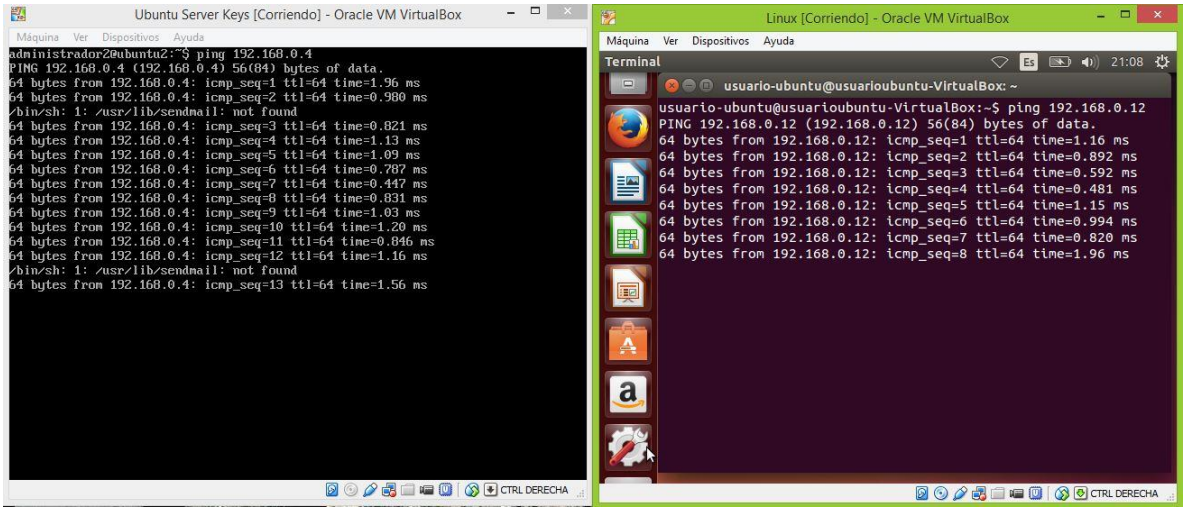


Fig.34. Comunicación de máquinas virtuales desde Ubuntu Server Keys (servidor) a Ubuntu Server SSH (servidor) y desde Ubuntu Server SSH (servidor) a Ubuntu Server Keys (servidor)

Comunicación entre sistemas operativos (departamentos de la empresa):

- Desde XP1 a Linux y desde Linux a XP1.

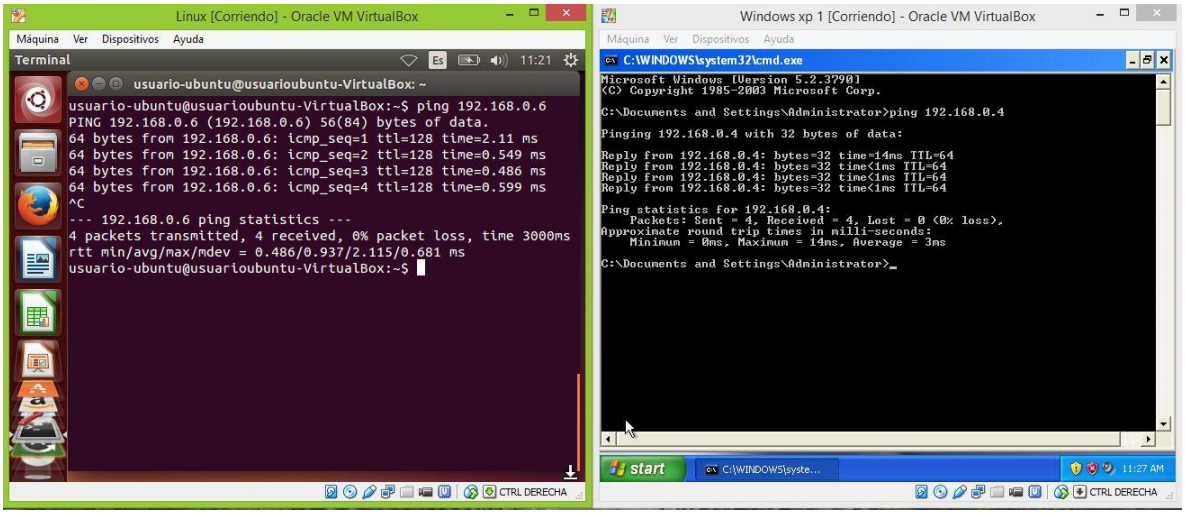


Fig.35. Comunicación de máquinas virtuales desde XP1 a Linux y desde Linux a XP1

- Desde XP2 a Linux y desde Linux a XP2.

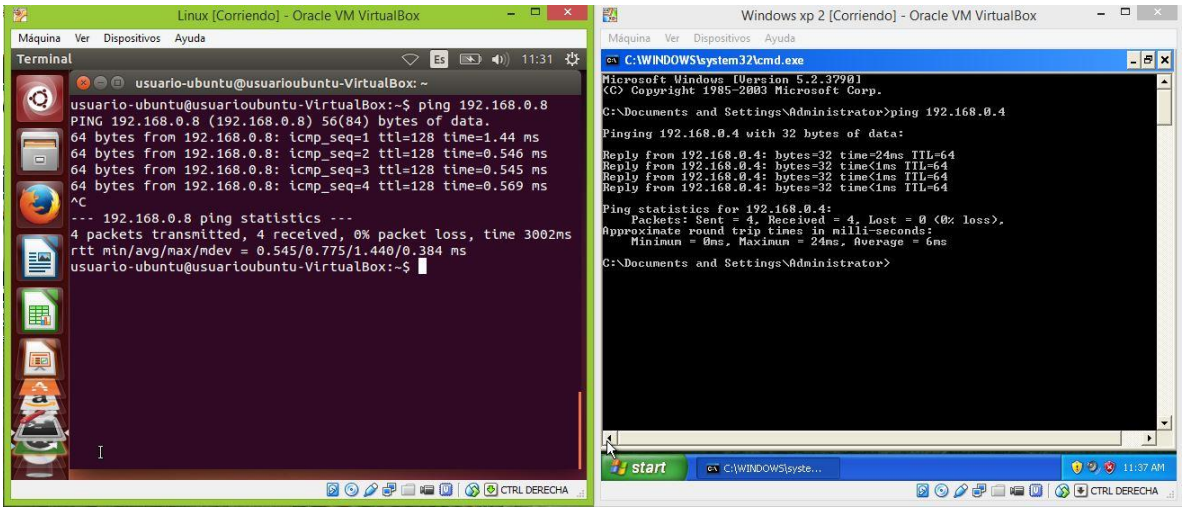


Fig.36. Comunicación de máquinas virtuales desde XP2 a Linux y desde Linux a XP2

- Desde XP1 a XP2 y desde XP2 a XP1.

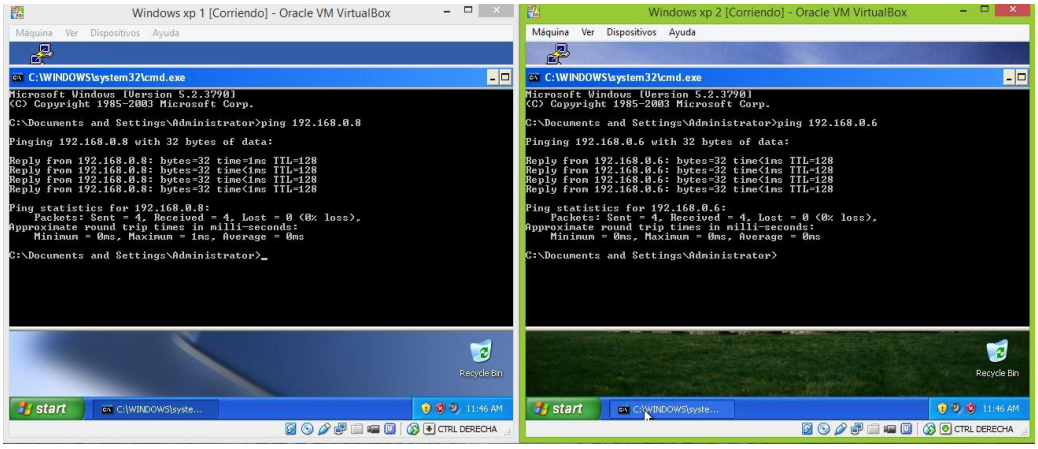


Fig.37. Comunicación de máquinas virtuales desde XP1 a XP2 y desde XP2 a XP1

CREACION DE GRUPOS, USUARIOS Y CARPETAS EN EL SERVIDOR SSH

Creación de Grupos en Ubuntu SSH Server:

1. Se ejecuta la máquina virtual Ubuntu Server SSH para realizar la creación de los grupos.

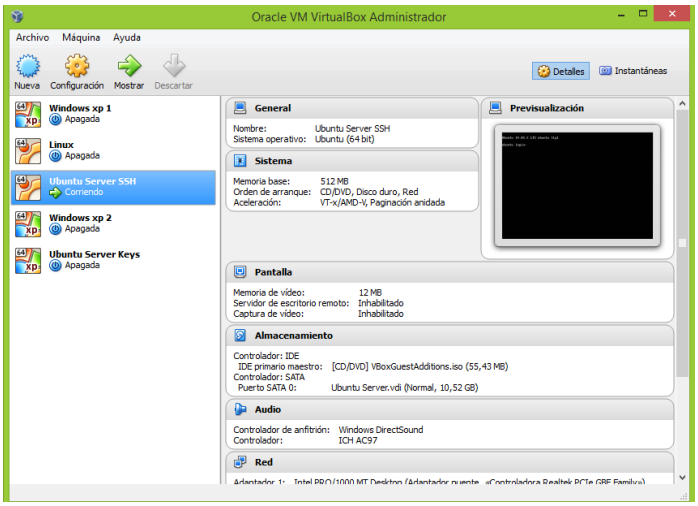


Fig.38. Interfaz de Virtualbox donde aparecen todas las máquinas virtuales

2. Se realiza el login para ingresar el procedimiento.

Fig.39. Proceso de Login de usuario en la consola de Ubuntu Server SSH

3. Se crea el grupo mediante el siguiente comando:

   Sudo addgroup (nombre del grupo)

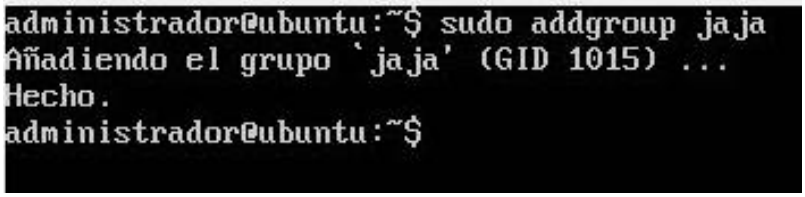


Fig.40. Proceso de creación de grupo en la consola de Ubuntu Server SSH

4. Se verifica que se haya creado el grupo ingresando a la carpeta raíz donde se creó mediante el siguiente comando (aparece el grupo seleccionado en en recuadro de color verde):

   Cat /ect/group

Creación de Usuarios en Ubuntu SSH Server:

1. Ya ingresando en el modo de consola de Ubuntu SSH Server se crea el usuario mediante el siguiente comando:
   Sudo adduser (nombre del usuario)

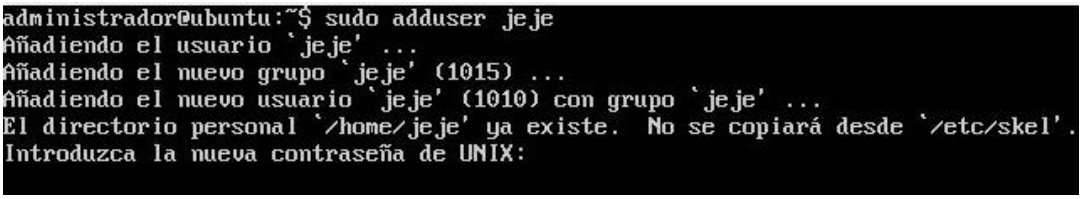


Fig.41. Proceso de creación de usuario en la consola de Ubuntu Server SSH

2. A continuación el sistema pedirá la contraseña propia de cada usuario la cual debe ser ingresada y confirmada:

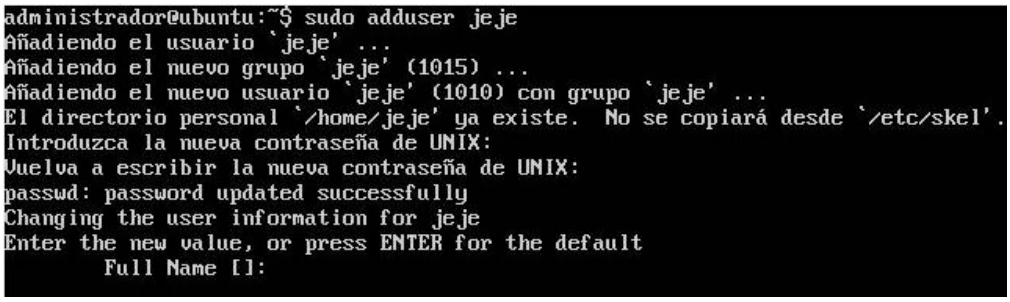


Fig.42. Proceso de asignación de contraseña al usuario en la consola de Ubuntu Server SSH

3. Ahora el sistema pedirá el nombre completo del usuario, número telefónico y datos que no son tan importantes para el proyecto. Luego el sistema preguntará si l información ingresada es correcta escribiendo S (si) o n (no):

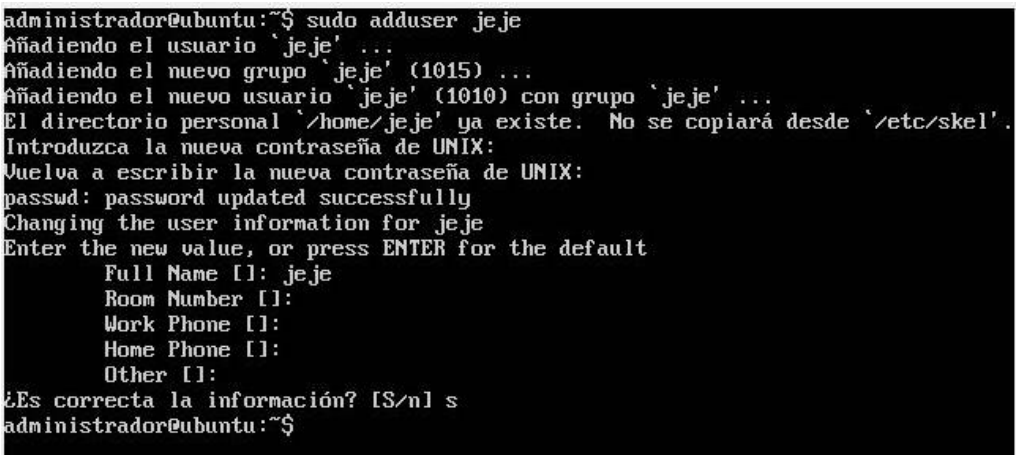


Fig.43. Proceso de confirmación de la información asignada al usuario en la consola de Ubuntu Server SSH

4. Por último se comprueba mediante el siguiente comando si se creó el usuario correctamente ingresando en primera instancia a la carpeta raíz donde se encuentra y luego verificando el usuario dentro de la misma:

Cd /home (comando para ingresar a la carpeta raíz)

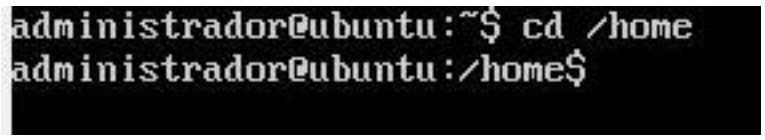


Fig.44. Proceso de ingreso a la carpeta raíz en la consola de Ubuntu Server SSH

Ls (comando para verificar el usuario dentro de la carpeta)

Fig.45. Proceso de verificación de la creación de usuario en la consola de Ubuntu Server SSH

También se puede verificar la información del usuario ingresado mediante el siguiente comando:

Cat /etc/passwd

Fig.46. Proceso de verificación de la creación de usuario en la consola de Ubuntu Server SSH

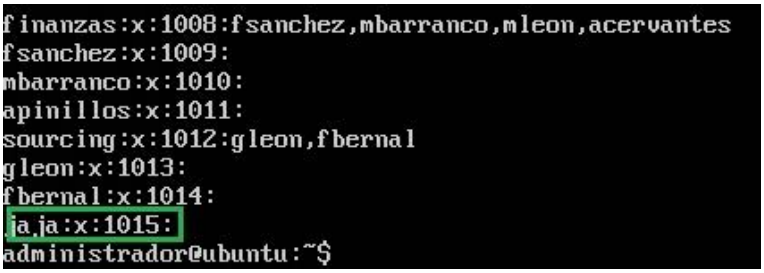


Fig.47. Proceso de verificación de la creación de usuario en la consola de Ubuntu Server SSH

Creación de Carpetas en Ubuntu SSH Server:

1. Para la creación de carpetas se necesita del siguiente comando:

   Sudo mkdir (nombre de la carpeta)

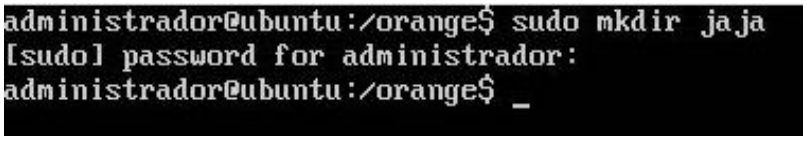


Fig.48. Proceso de creación de carpetas en la consola de Ubuntu Server SSH

2. Una vez creada la carpeta se verifica su ubicación mediante el siguiente comando (se comprueba en la imagen resaltada en el recuadro verde):

Ls (comando para verificar la creación de la carpeta dentro de la carpeta raíz)

Fig.49. Proceso de verificación de la creación de las carpetas en la consola de Ubuntu Server SSH

Vinculación de Usuarios a Grupos en Ubuntu SSH Server:

1. Teniendo ya creados los grupos y usuarios se pueden vincular mediante el siguiente comando:

Sudo adduser (nombre del usuario) (nombre del grupo)

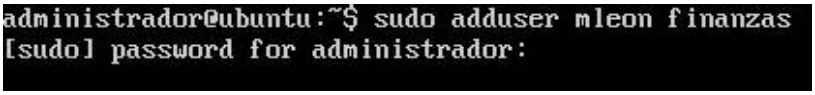


Fig.50. Proceso de vinculación de usuarios a grupos en la consola de Ubuntu Server SSH

2. Una vez vinculado un usuario a un grupo determinado, se verifica que haya quedado correctamente mediante el siguiente comando:

Cat /etc/group

Fig.51. Proceso de verificación de la vinculación de los usuarios a grupos en la consola de Ubuntu Server SSH

INSTALACIÓN DEL PAQUETE SKS-KEYSERVER (OPEN PGP) EN UBUNTU SERVER KEYS

Para implementar el servidor de llaves públicas de los usuarios destinadas al proceso de encriptación y des-encriptación de archivos, es necesario instalar el servidor SKS-KEYSERVER que es un servidor OPENPGP, cuya función es la sincronización de llaves públicas de manera sencilla, descentralizada y confiable.

1. Primero se instala el servidor SKS-KEYSERVER mediante el siguiente comando:

   Sudo apt-get –y install sks

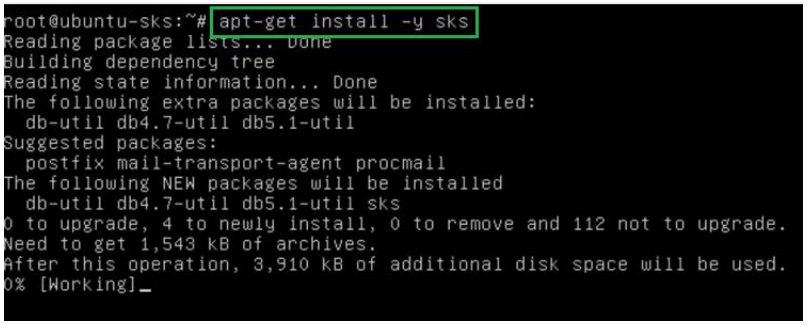


Fig.52. Proceso de instalación del servidor de llaves SKS-KEYSERVER en Ubuntu Server Keys

2. Ahora se crea la base de datos mediante el siguiente comando:

   Sudo sks build

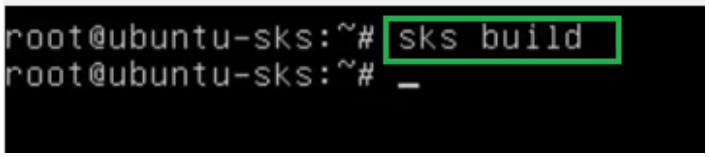


Fig.53. Proceso de creación de la base de datos del servidor de llaves SKS-KEYSERVER en Ubuntu Server Keys

3. A continuación se deben cambiar los permisos de la base datos anteriormente creada para que se pueda escribir en ella mediante el siguiente comando:

   Sudo chown –Rc debían-sks:debían-sks /var/libsks/DB

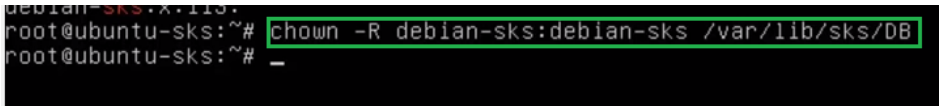


Fig.54. Proceso de asignación de permisos de escritura a la base de datos del servidor de llaves SKS-KEYSERVER en Ubuntu Server Keys

4. Como el servicio se debe inicializar al momento de iniciar la máquina virtual Ubuntu Server Keys, se modifica el archivo /etc/default/sks mediante el siguiente comando:

Sudo vi /etc/default/sks

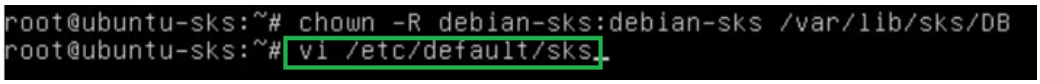


Fig.55. Proceso de modificación del archivo sks del servidor de llaves SKS-KEYSERVER en Ubuntu Server Keys

El parámetro a cambiar en el archivo inicialmente aparece en *NO* de manera que se cambia de la siguiente forma:

Initstart= yes

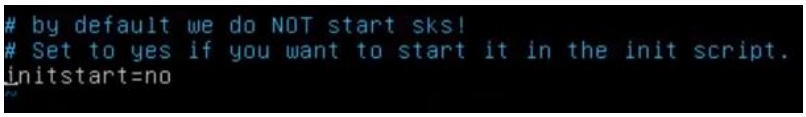


Fig.56. Archivo /etc/default/sks (sin modificar)

Fig57. Archivo /etc/default/sks (modificado)

5. Por último se inicializa el servicio sks mediante el siguiente comando:

/etc/init.d/sks start

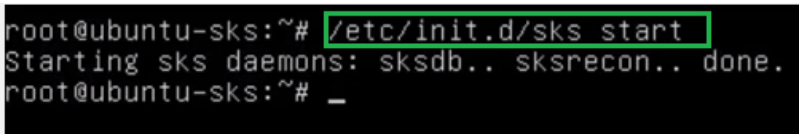


Fig.58. Proceso de inicialización del servidor de llaves SKS-KEYSERVER en Ubuntu Server Keys

CREACION DE LLAVES PÚBLICA Y PRIVADA (PARA EL PROCESO DE ENCRIPTACION DES-ENCRIPTACIÓN DE ARCHIVOS)

Teniendo en cuenta que en el proyecto se manejarán dos sistemas operativos diferentes que son Windos XP (Departamentos de Ventas y Finanzas) y Ubuntu Linux (Departamento de

Operaciones), se manejarán dos procesos diferentes en la creación de las llaves públicas y privadas que son necesarias para el proceso de encriptación y des-encriptación que brinda mayor seguridad en el manejo y manipulación de archivos.

Creación de llaves pública y privada con GNUPG (Modo gráfico de generación de llaves):

1. Primero se ingresa a la aplicación del sistema operativo Linux "Contraseñas y claves".

Fig.59. Ingreso a la aplicación Contraseñas y claves desde el usuario Linux (Departamento de Operaciones)

2. En la aplicación, se da click en el ícono en forma de cruz en la parte superior de la pantalla y se selecciona la opción "Clave PGP" para la creación de las llaves pública y privada.

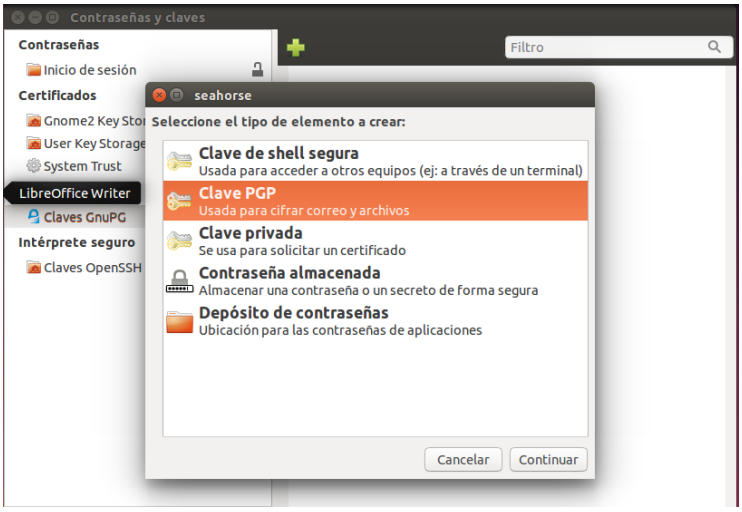


Fig.60. Creación de las llaves pública y privada en la aplicación Contraseñas y claves desde el usuario Linux (Departamento de Operaciones)

3. A continuación se abrirá una ventana en la que pedirá agregar la siguiente información:

Nombre completo (Obligatorio)
Dirección de correo (No es obligatorio)
Tipo de cifrado (Obligatorio)
Fortaleza de la clave (Obligatorio)
Fecha de caducidad (Obligatorio)

Después de ingresar la información solicitada se da click en el icono "Crear".

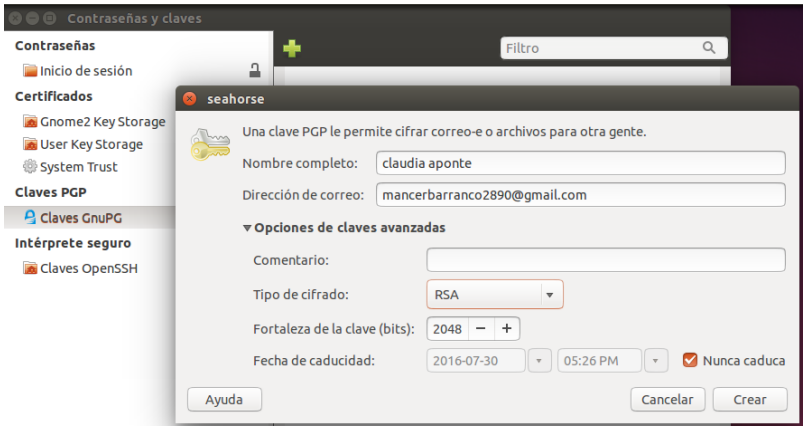


Fig.61. Creación de las llaves pública y privada en la aplicación Contraseñas y claves desde el usuario Linux (Departamento de Operaciones)

4. Ahora el sistema pedirá ingresar una contraseña que protege de mejor manera las llaves pública y privada al momento de su uso. Se asigna una contraseña que sea fácil de recordar.

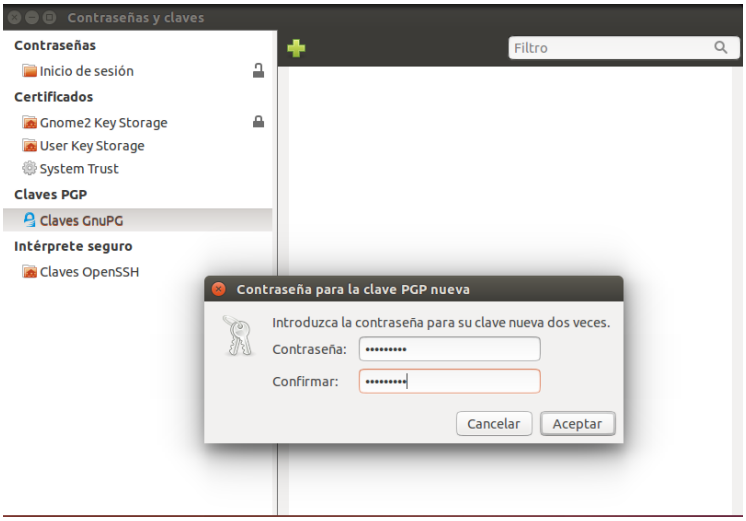


Fig.62. Asignación de contraseña de protección a las llaves pública y privada en la aplicación Contraseñas y claves desde el usuario Linux (Departamento de Operaciones)

5. Ya realizado el proceso anterior, se revisa que hayan sido creadas las llaves pública y privada en el directorio indicado:

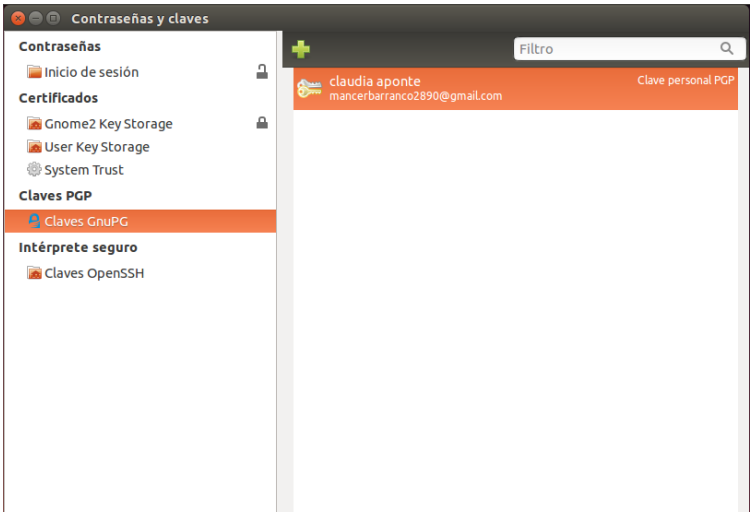


Fig.63. Verificación de las llaves pública y privada creadas en la aplicación Contraseñas y claves desde el usuario Linux (Departamento de Operaciones)

Creación de llaves pública y privada con GNUPG (Generación de las llaves por consola):

1. Primero generamos las llaves pública y privada mediante el siguiente comando:

Gpg -- gen-key

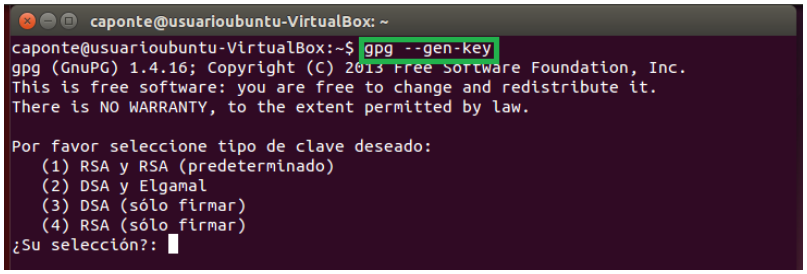


Fig.64. Creación de las llaves pública y privada en la consola desde el usuario Linux (Departamento de Operaciones)

2. Ahora el sistema pedirá seleccionar el tipo de llave que se desea crear, de manera que elegimos la siguiente opción:

(1) RSA Y RSA (PREDETERMINADO)

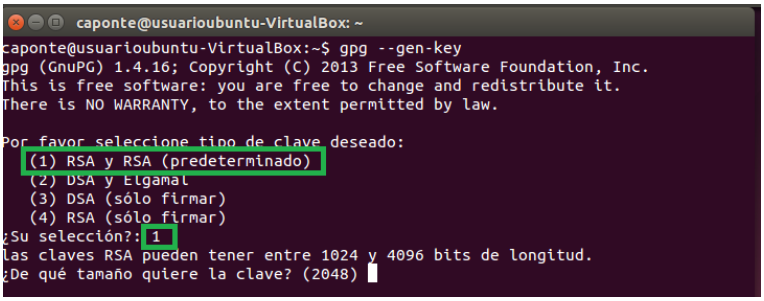


Fig.65. Creación de las llaves pública y privada en la consola desde el usuario Linux (Departamento de Operaciones)

3. Después el sistema pedirá el tamaño de las llaves pública y privada entre 1024 y 4096 bits de longitud, para el caso del proyecto se elegirá la opción 2048 bits la cuál es segura y un poco más rápida en su creación.

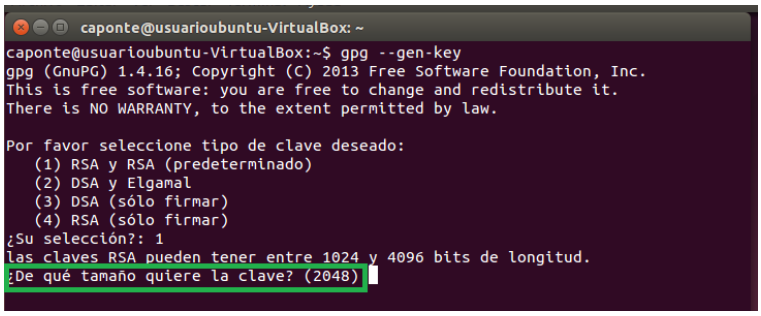


Fig.66. Creación de las llaves pública y privada en la consola desde el usuario Linux (Departamento de Operaciones)

4. A continuación el sistema pedirá especificar el periodo de validez de las llaves pública y privada con el fin de garantizar la seguridad de las mismas, para el caso del proyecto se seleccionará la siguiente opción:

0 = la clave nunca caduca

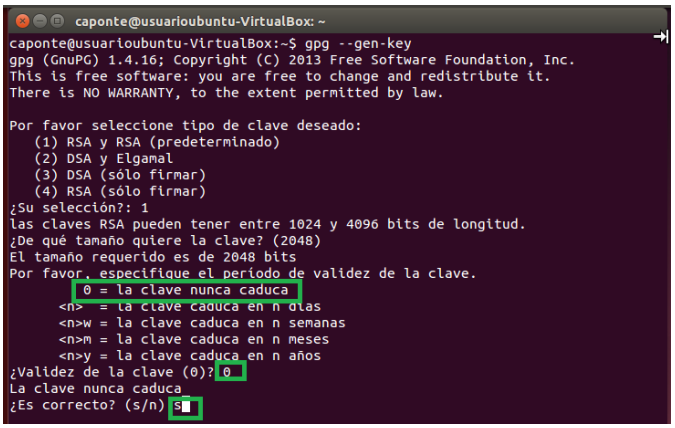


Fig.67. Creación de las llaves pública y privada en la consola desde el usuario Linux (Departamento de Operaciones)

5. Teniendo realizado el proceso anterior, el sistema solicitará el ingreso de información como lo es el nombre completo (Obligatorio) y dirección de correo electrónico (No es obligatorio).

   Por último el sistema pedirá la confirmación del usuario si la información ingresada es correcta por lo que se ingresará la letra "v" para continuar con el proceso.

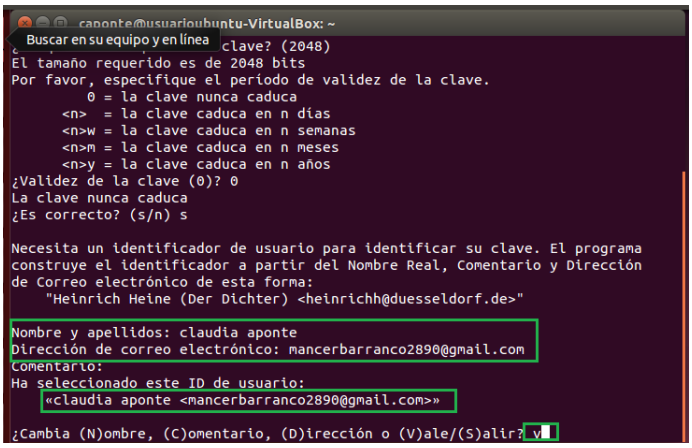


Fig.68. Creación de las llaves pública y privada en la consola desde el usuario Linux (Departamento de Operaciones)

6. Tal como en el modo gráfico de generación de llaves el sistema pedirá el ingreso de una contraseña para brindar mayor seguridad a las mismas. Luego se dará click en el icono "Desbloquear" para continuar con el proceso.

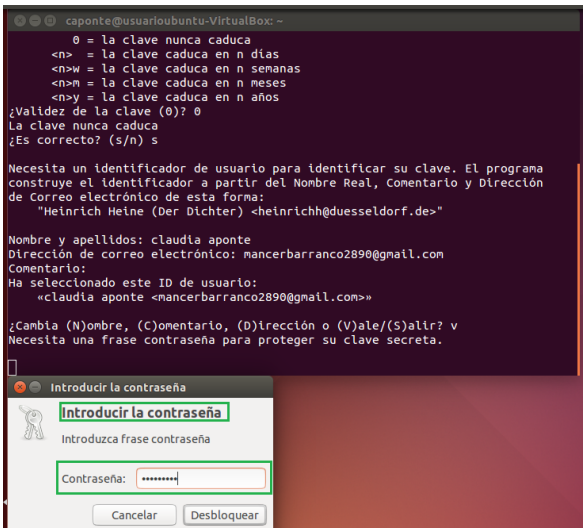


Fig.69. Creación de las llaves pública y privada en la consola desde el usuario Linux (Departamento de Operaciones)

7. Por último el sistema pedirá realizar trabajos en carpetas, archivos o movimientos con mouse para generar entropía y así tener bytes para crear las llaves públicas y privadas.

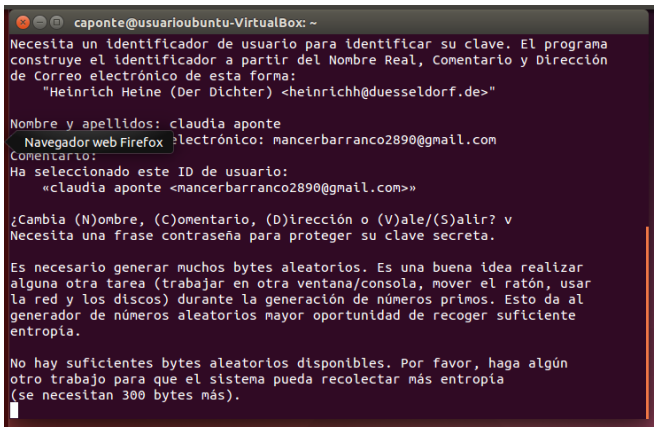


Fig.70. Creación de las llaves pública y privada en la consola desde el usuario Linux (Departamento de Operaciones)

8. Ya creadas las llaves pública y privada se verifican en consola donde aparecen como pub (llave pública) y sub (llave privada).

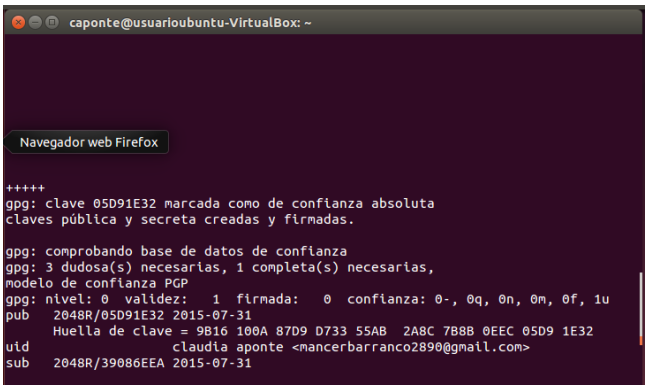


Fig.71. Creación de las llaves pública y privada en la consola desde el usuario Linux (Departamento de Operaciones)

También se pueden verificar las llaves pública y privada creadas mediante el siguiente comando:

Gpg – list-keys

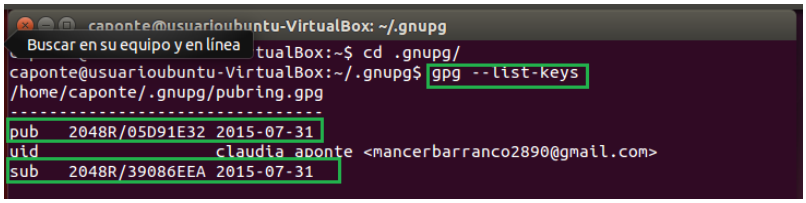


Fig.72. Verificación de las llaves pública y privada creadas en la consola desde el usuario Linux (Departamento de Operaciones)

9. Si se desea verificar la creación de las llaves pública y privada, ingresamos el comando:

Seahorse

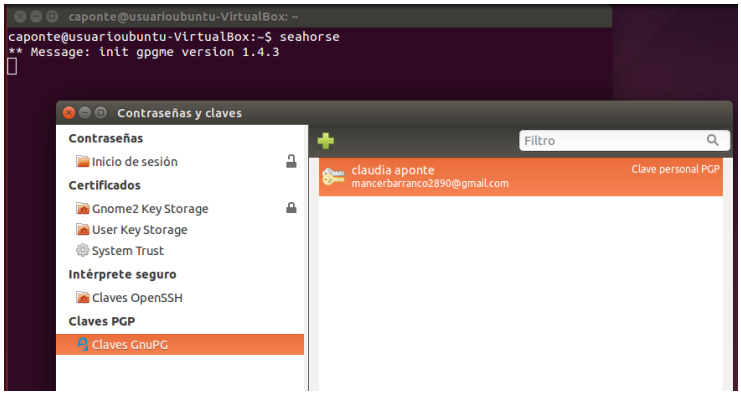


Fig.73. Verificación de las llaves pública y privada creadas en la consola desde el usuario Linux (Departamento de Operaciones)

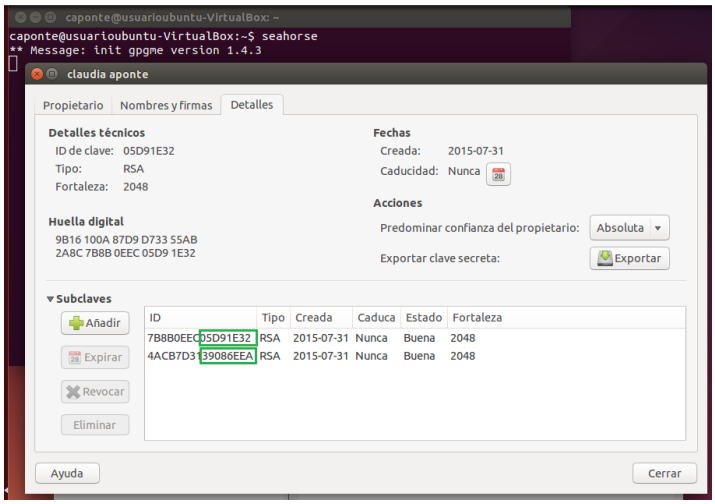


Fig.74. Verificación de las llaves pública y privada creadas en la consola desde el usuario Linux (Departamento de Operaciones)

ALMACENAMIENTO DE LLAVES PÚBLICAS DESDE EL USUARIO LINUX (DEPARTAMENTO DE OPERACIONES) AL SERVIDOR UBUNTU SERVER KEYS

1. Primero se revisa el ID de la llave pública mediante el siguiente comando:

   Gpg – list-keys

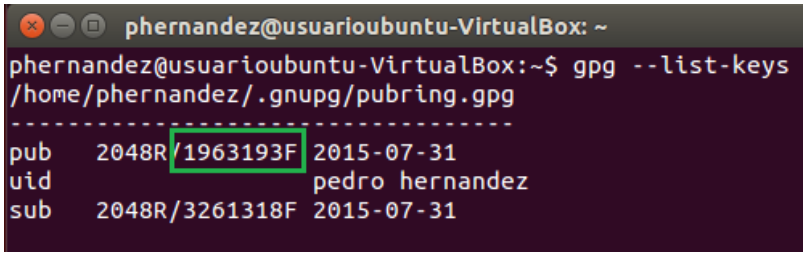


Fig.75. Verificación de las llaves pública y privada creadas en la consola desde el usuario Linux (Departamento de Operaciones)

2. A continuación se escribe el siguiente comando para cargar la llave pública desde el cliente al servidor de llaves:

   Gpg – send-keys – keyserver (dirección IP del servidor Ubuntu Server Keys) (ID de la llave pública que se va a almacenar)

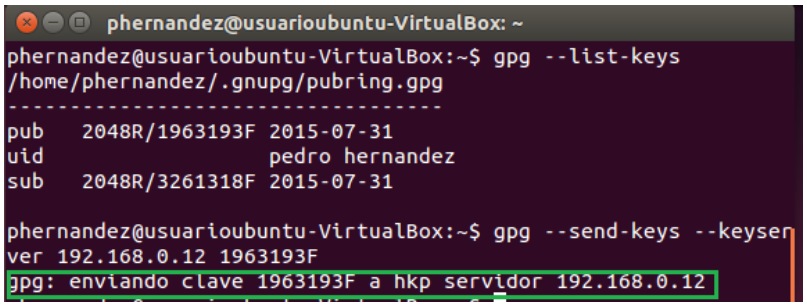


Fig.76. Almacenamiento de la llave pública creada en la consola desde el usuario Linux (Departamento de Operaciones) al servidor Ubuntu Server Keys

ENCRIPTACIÓN Y ALMACENAMIENTO DE ARCHIVOS EN EL REPOSITORIO SSH

1. Se crea un archivo de cualquier tipo para ser encriptado, en este caso será un archivo de texto creado en el editor de texto de Linux "nano" que tendrá como nombre "prueba1".

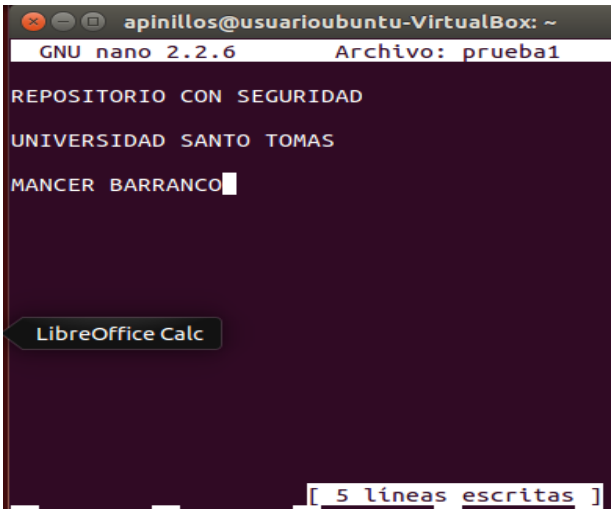


Fig.77. Creación del archivo a encriptar en la consola del usuario Linux (Departamento de Operaciones)

2. A continuación se verifica en las carpetas del usuario la creación del archivo.

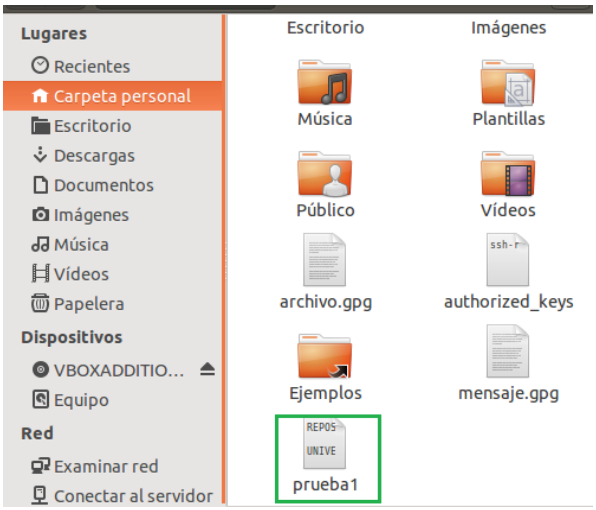


Fig.78. Verificación de la creación del archivo a encriptar en la consola del usuario Linux (Departamento de Operaciones)

3. A continuación se descarga la llave pública del usuario que requiera ver la información del archivo desde el Server Keys mediante el siguiente comando:

Gpg --keyserver (dirección IP del Server Keys) –recv-keys (ID de la llave pública del usuario que requiera ver la información).

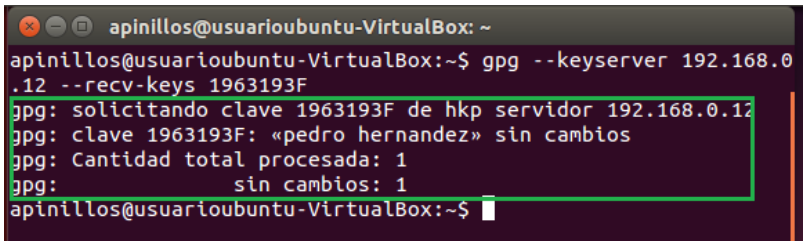


Fig.79. Descarga de la llave pública del usuario que requiere ver la información desde el servidor Ubuntu Server Keys al usuario Linux (Departamento de Operaciones)

4. Se verifica que la llave pública haya sido descargada mediante el siguiente comando:

Gpg --list-keys.

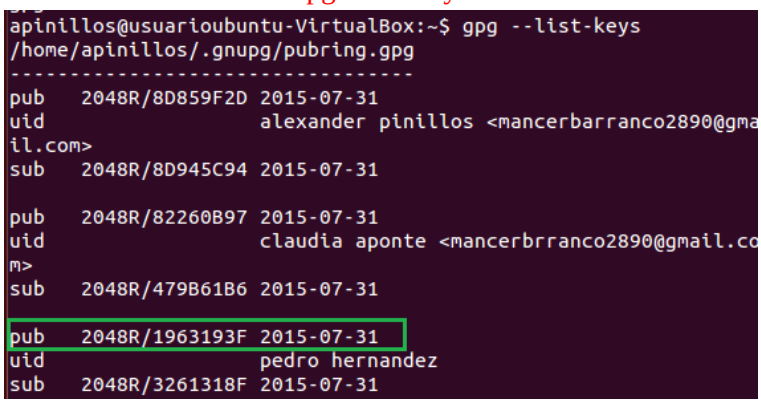


Fig.80. Verificación de la descarga de la llave pública del usuario que requiere ver la información desde el servidor Ubuntu Server Keys al usuario Linux (Departamento de Operaciones)

5. Ahora se encripta el archivo con la llave pública del usuario que requiere ver la información para el caso del ejemplo el usuario pedro hernandez, mediante el siguiente comando:

Gpg --encrypt --recipient (ID de la llave pública del usuario que requiera ver la información) (nombre del archivo que se va a encriptar).

Luego de esto el sistema pedirá la confirmación del usuario si desea usar la clave pública para encripta, donde se escribirá "S" para continuar con el proceso.

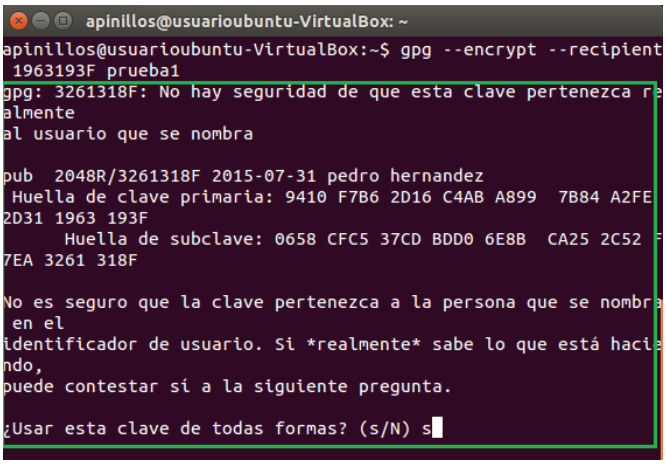


Fig.81. Proceso de confirmación de uso de la llave pública del usuario Linux (Departamento de Operaciones) para encriptar el archivo prubea1

6. Se verifica si el archivo fue encriptado con la llave pública, revisando si se ha creado un archivo con la extensión de encriptación (.gpg) y que al abrirlo no contenga el mensaje o información que se desea ocultar.

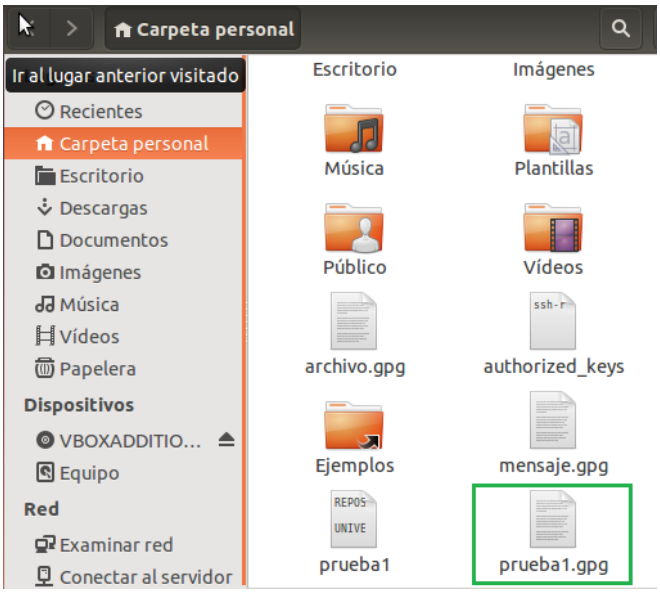


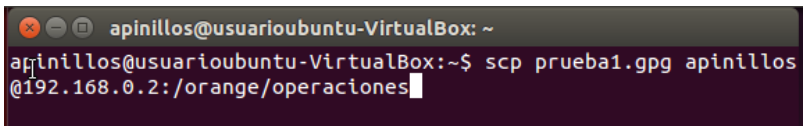
Fig.82. Proceso de verificación del archivo encriptado por el usuario Linux (Departamento de Operaciones)

Fig.83. Proceso de verificación del archivo encriptado por el usuario Linux (Departamento de Operaciones)

7. Ahora se almacena el archivo encriptado al repositorio con seguridad o Server SSH mediante el siguiente comando:

Scp (nombre del archivo.gpg) (nombre del usuario)@(dirección IP del Server SSH): (ubicación o carpeta en la que se almacenará al archivo encriptado).

El sistema pedirá introducir la contraseña privada del usuario asignada en el proceso de generación de las llaves para continuar con el proceso.



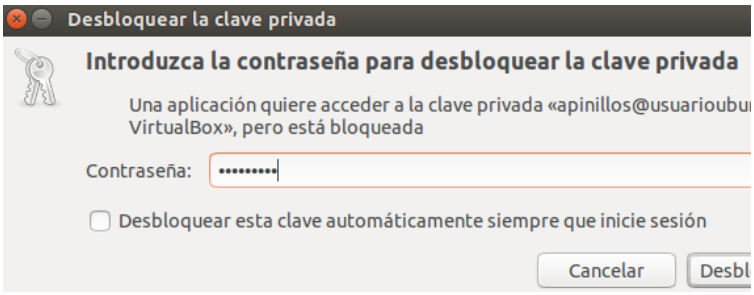


Fig.84. Proceso de almacenamiento del archivo encriptado desde el usuario Linux (Departamento de Operaciones) al repositorio Ubuntu Server SSH

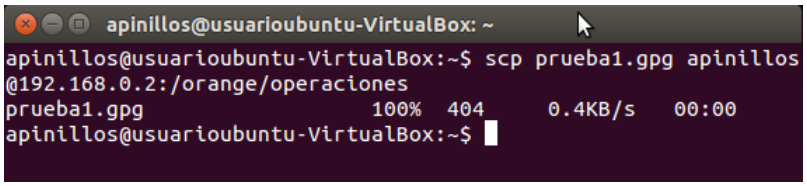


Fig.85. Proceso de almacenamiento del archivo encriptado desde el usuario Linux (Departamento de Operaciones) al repositorio Ubuntu Server SSH

8. Por último, se verifica el archivo almacenado en la ubicación asignada dentro del repositorio o Server SSH.

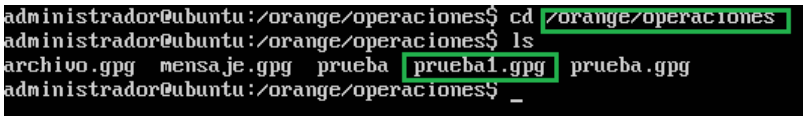


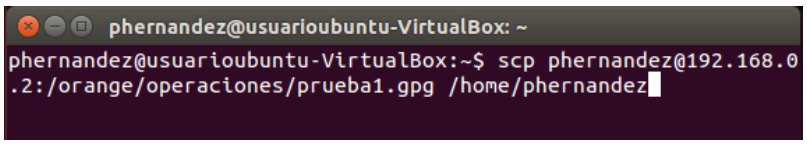
Fig.86. Proceso de verificación de almacenamiento del archivo encriptado al repositorio Ubuntu Server SSH

DESCARGA Y DES-ENCRIPTACIÓN DE ARCHIVOS DEL REPOSITORIO UBUNTU SERVER SSH A LOS USUARIOS LINUX (DEPARTAMENTO DE OPERACIONES)

1. Para descargar el archivo encriptado desde el repositorio Ubuntu Server SSH, se ingresa el siguiente comando en la consola del usuario que requiera el archivo:

Scp (nombre del usuario)@(dirección IP del Server SSH): (ubicación o carpeta en la que se almacenó el archivo encriptado en el repositorio o Server SSH, incluyendo el archivo con la extensión .gpg) (ubicación o carpeta del usuario donde se requiere almacenar y des-encriptar)

El sistema pedirá introducir la contraseña privada del usuario asignada en el proceso de generación de las llaves para continuar con el proceso.



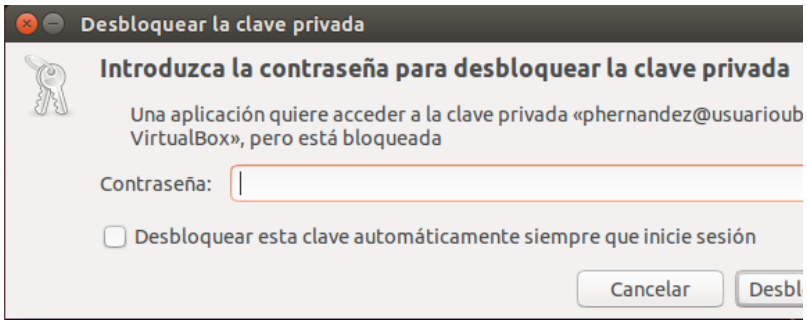


Fig.87. Proceso de descarga del archivo encriptado desde el repositorio Ubuntu Server SSH al usuario Linux (Departamento de Operaciones)

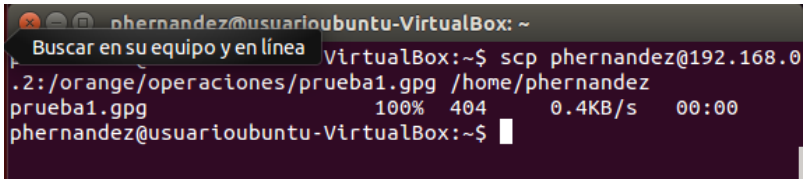


Fig.88. Proceso de descarga del archivo encriptado desde el repositorio Ubuntu Server SSH al usuario Linux (Departamento de Operaciones)

2. Se verifica que el archivo haya sido almacenado correctamente en la ubicación asignada:

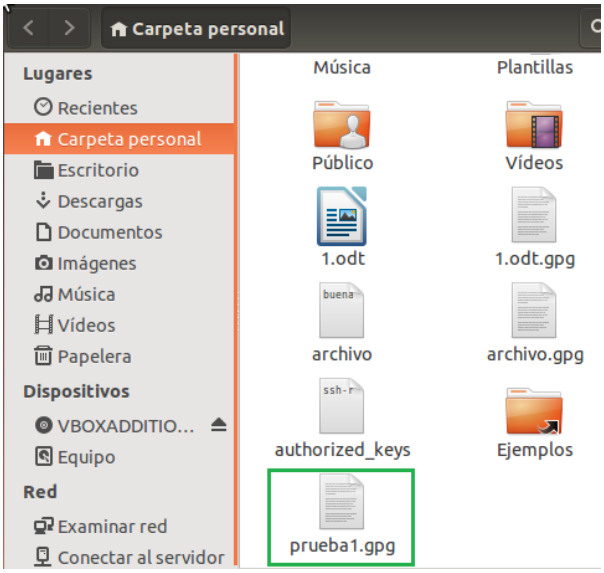


Fig.89. Proceso de verificación de la descarga del archivo encriptado desde el repositorio Ubuntu Server SSH al usuario Linux (Departamento de Operaciones)

3. Ahora se realiza el proceso de des-encriptación del archivo encriptado introduciendo en consola el siguiente comando:

Gpg –d (nombre del archivo).gpg

El sistema pedirá introducir la contraseña privada del usuario asignada en el proceso de generación de las llaves para continuar con el proceso.

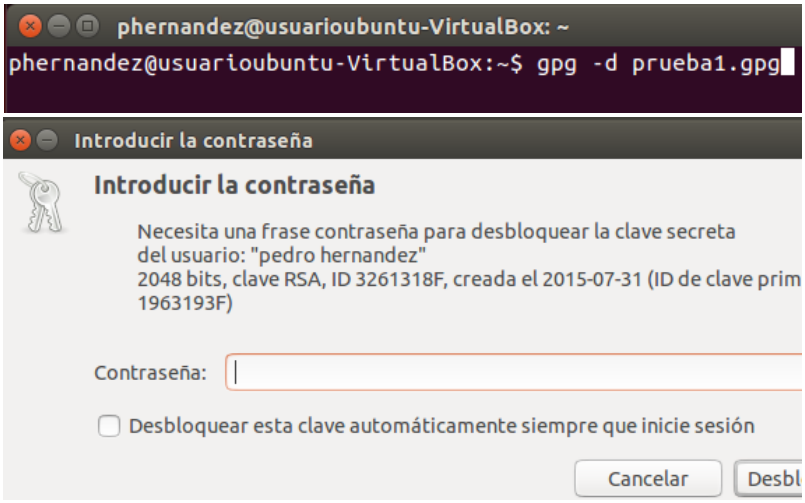


Fig.90. Proceso de ingreso de la contraseña de usuario para des-encriptación del archivo prueba1

4. Por último, el archivo es des-encriptado correctamente y se puede visualizar la información que el usuario desea.

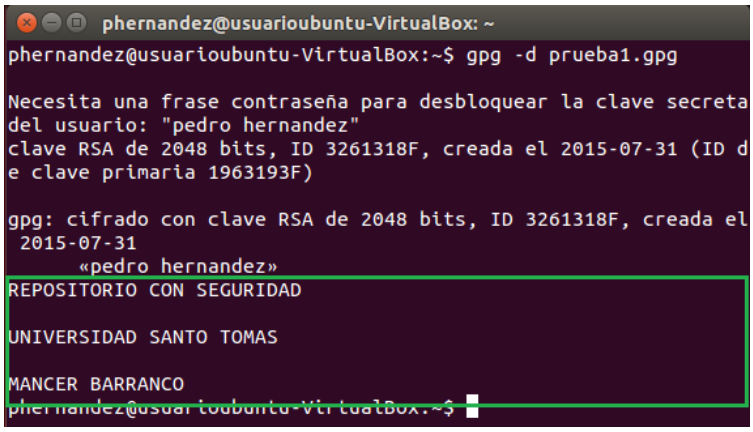


Fig.91. Proceso de verificación del archivo des-encriptado mediante el uso de la llave privada del usuario Linux (Departamento de Operaciones)

INSTALACIÓN DE LA APLICACIÓN GPG4WIN (SOFTWARE LIBRE KLEOPATRA)

Teniendo en cuenta que el sistema operativo XP maneja diferentes procedimientos para la creación de llaves públicas y privadas que se utilizan para el proceso de encriptación y des-encriptación de archivos, es necesario instalar la aplicación GPG4WIN que contiene el software libre Kleopatra utilizado para este procedimiento. A continuación se indicará el procedimiento para su instalación en cada uno de los sistemas operativos Windows XP1 y XP2 (Departamento de ventas y finanzas):

1. Primero se ejecuta la aplicación gpg4win-2.2.5.

Fig.92. Proceso de instalación de la aplicación GPG4WIN - Imagen tomada de: http://es.slideshare.net/8enja/kleo

2. Se hace click en el icono "siguiente".

Fig.93. Proceso de instalación de la aplicación GPG4WIN- Imagen tomada de: http://es.slideshare.net/8enja/kleo

3. Se hace click en el icono "siguiente" para aceptar el acuerdo de licencia.

Fig.94. Proceso de instalación de la aplicación GPG4WIN - Imagen tomada de: http://es.slideshare.net/8enja/kleo

4. A continuación se realiza la selección de todos los componentes de la aplicación excepto "Claws-Mail".

Fig.95. Proceso de instalación de la aplicación GPG4WIN - Imagen tomada de: http://es.slideshare.net/8enja/kleo

5. Luego se hace click en el icono "siguiente" para continuar con la instalación.

Fig.96. Proceso de instalación de la aplicación GPG4WIN - Imagen tomada de: http://es.slideshare.net/8enja/kleo

6. Ahora se hace click en el icono “siguiente”.

Fig.97. Proceso de instalación de la aplicación GPG4WIN- Imagen tomada de: http://es.slideshare.net/8enja/kleo

7. Se hace click en el icono “instalar”.

Fig.98. Proceso de instalación de la aplicación GPG4WIN- Imagen tomada de: http://es.slideshare.net/8enja/kleo

8. Se espera a que la aplicación se instale y se hace click en el icono "siguiente".

Fig.99. Proceso de instalación de la aplicación GPG4WIN - Imagen tomada de: http://es.slideshare.net/8enja/kleo

9. Ahora se selecciona la casilla "Root certificate defined or skip configuration" y se da click en el icono "siguiente."

Fig.100. Proceso de instalación de la aplicación GPG4WIN - Imagen tomada de: http://es.slideshare.net/8enja/kleo

10. Por último se hace click en el icono "terminar" para finalizar con la instalación de la aplicación.

Fig.101. Proceso de instalación de la aplicación GPG4WIN - Imagen tomada de: http://es.slideshare.net/8enja/kleo

11. Para corroborar que la aplicación haya sido instalada correctamente, se ejecuta el software libre Kleopatra y debe abrirse una ventana similar a la de la figura a continuación:

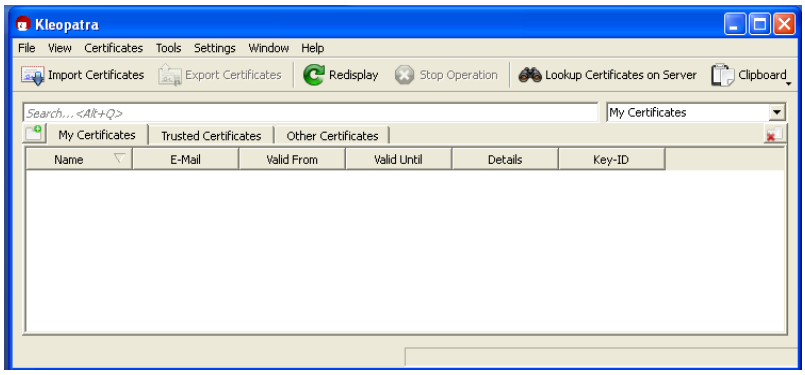


Fig.102. Proceso de verificación de la instalación de la aplicación GPG4WIN (Software libre Kleopatra)

CREACIÓN DE LLAVES PÚBLICA Y PRIVADA (PROCESO DE ENCRIPTACIÓN Y DES-ENCRIPTACIÓN DE ARCHIVOS PARA USUARIOS XP)

A continuación se describirá el proceso de generación de las llaves públicas y privadas para encriptar y des-encriptar los archivos manejados en los departamentos de Ventas y Finanzas.

1. Primero se ejecuta el programa Kleopatra y se da click en el icono "File".

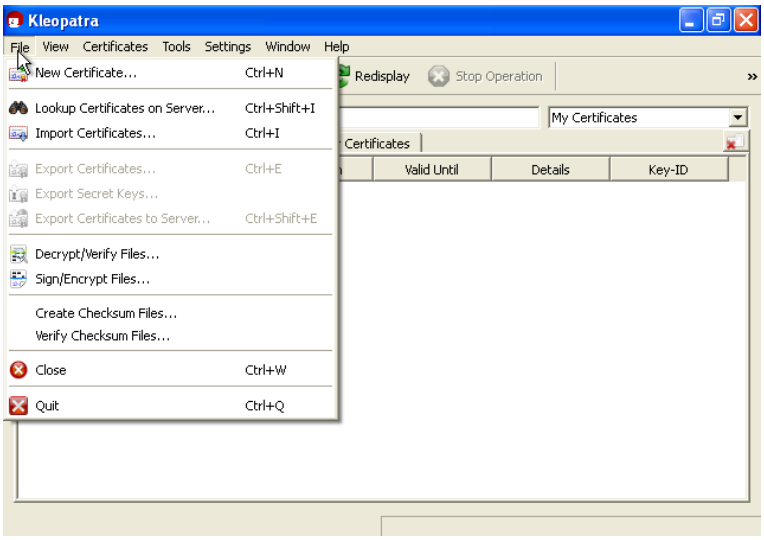


Fig.103. Proceso de generación de las llaves pública y privada en el programa Kleopatra para clientes Windows XP1 y XP2 (Departamentos de Ventas y Finanzas)

2. Ahora se selecciona la opción "Create a Personal OpenPGP Key pair".

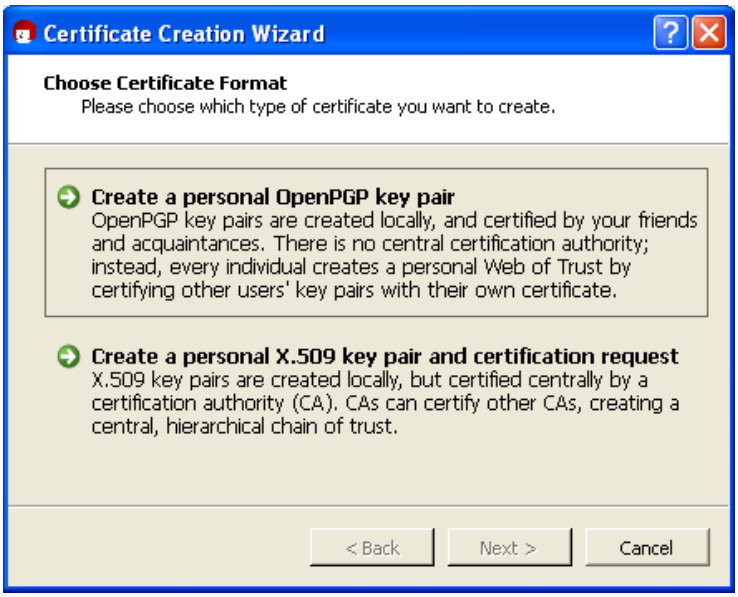


Fig.104. Proceso de generación de las llaves pública y privada en el programa Kleopatra para clientes Windows XP1 y XP2 (Departamentos de Ventas y Finanzas)

3. A continuación se agrega la siguiente información personal del usuario:

   Nombre (Obligatorio)
   Dirección de correo electrónico (Obligatorio)
   Comentarios (Opcional)

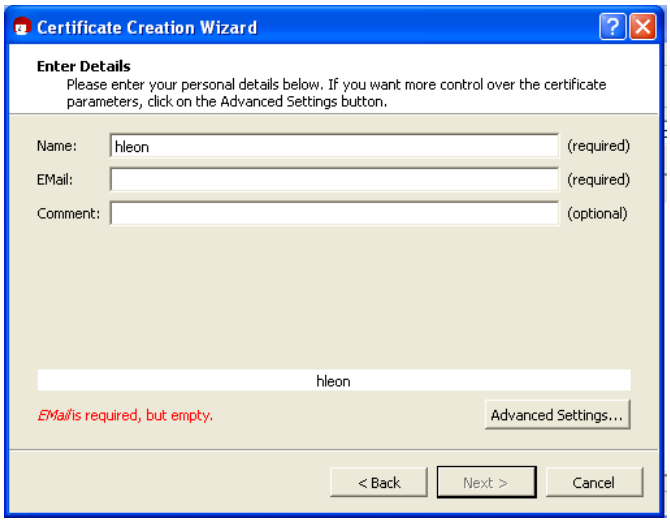


Fig.105. Proceso de generación de las llaves pública y privada en el programa Kleopatra para clientes Windows XP1 y XP2 (Departamentos de Ventas y Finanzas)

4. En seguida de este procedimiento, se da click en el icono "Advanced Settings" y se seleccionan los siguientes detalles técnicos que se encuentran por defecto y se adaptan al proyecto:

RSA (2048 bits) (Obligatorio)

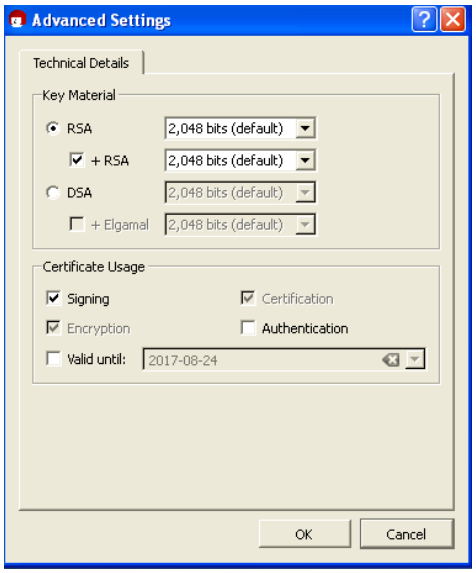


Fig.106. Proceso de generación de las llaves pública y privada en el programa Kleopatra para clientes Windows XP1 y XP2 (Departamentos de Ventas y Finanzas)

5. Para continuar, se da click en el icono “Next” para que el usuario verifique la información ingresada anteriormente antes de crear las llaves pública y privada.

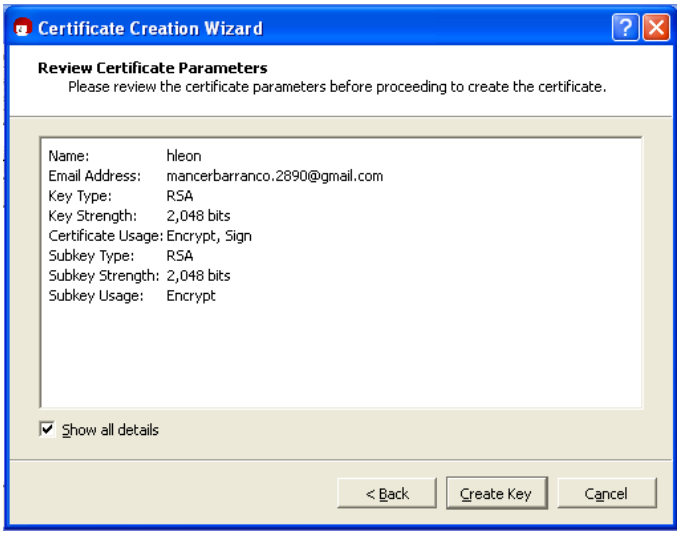


Fig.107. Proceso de generación de las llaves pública y privada en el programa Kleopatra para clientes Windows XP1 y XP2 (Departamentos de Ventas y Finanzas)

6. Después se da click en el icono “Create Key” donde pedirá ingresar una contraseña (Passphrase) preferiblemente que sea de fácil de recordar, para proteger las llaves pública y privada generadas.

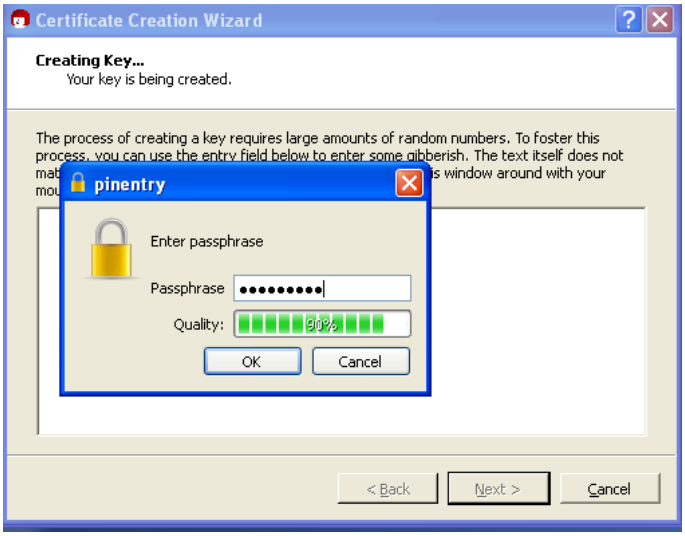


Fig.108. Proceso de generación de las llaves pública y privada en el programa Kleopatra para clientes Windows XP1 y XP2 (Departamentos de Ventas y Finanzas)

7. El sistema pedirá re ingresar la contraseña (Passphrase) escrita anteriormente. Luego se da click en el icono "OK" para continuar con el proceso.

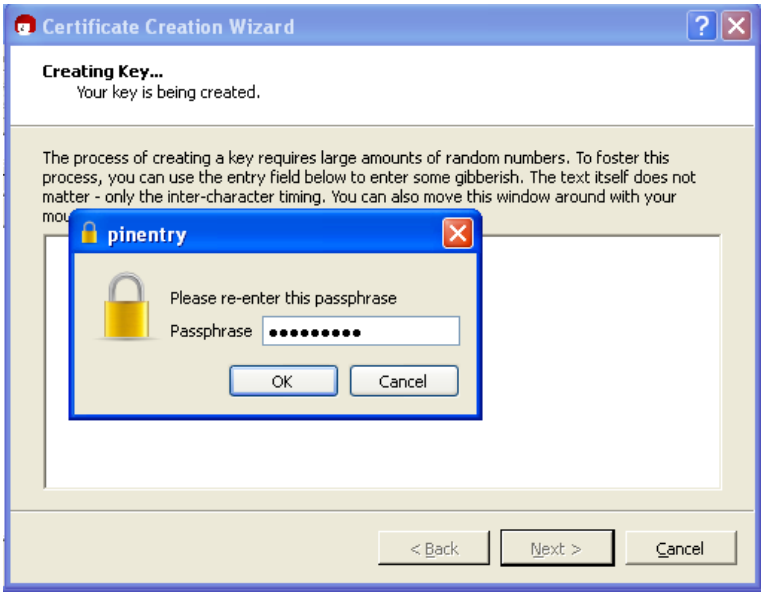


Fig.109. Proceso de generación de las llaves pública y privada en el programa Kleopatra para clientes Windows XP1 y XP2 (Departamentos de Ventas y Finanzas)

8. Por último el sistema confirmara la creación de las llaves pública y privada.

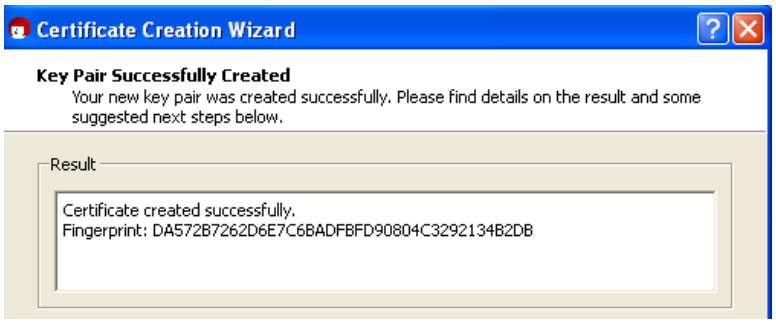


Fig.110. Proceso de generación de las llaves pública y privada en el programa Kleopatra para clientes Windows XP1 y XP2 (Departamentos de Ventas y Finanzas)

Se podrán verificar las llaves públicas y privadas en la siguiente ventana emergente, donde aparecerán los identificadores (Key-ID) que distinguen la llave pública (Parte superior) y llave privada (Parte inferior).

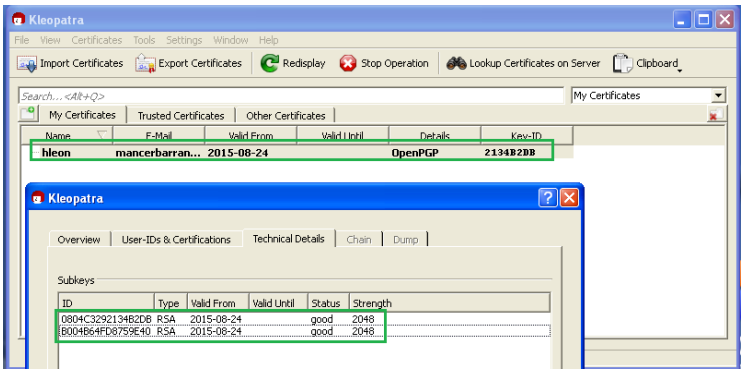


Fig.111. Proceso de generación de las llaves pública y privada en el programa Kleopatra para clientes Windows XP1 y XP2 (Departamentos de Ventas y Finanzas)

ALMACENAMIENTO DE LLAVE PÚBLICA DESDE EL USUARIO AL SERVIDOR UBUNTU SERVER KEYS (PARA USUARIOS WINDOWS XP1 Y XP2)

Teniendo las llaves públicas y privadas generadas, ahora se almacenan las llaves públicas en el servidor Ubuntu Server Keys para el proceso de encriptación de archivos.

1. Teniendo ejecutada la máquina virtual Ubuntu Server Keys e inicializando el servidor de llaves SKS-KEYSERVER para el almacenamiento de las llaves públicas, se da click en el icono de la ventana de la barra de herramientas “Settings” y luego en el icono “Configure Kleopatra” para configurar la comunicación entre el servidor Ubuntu Server Keys y el programa Kleopatra.

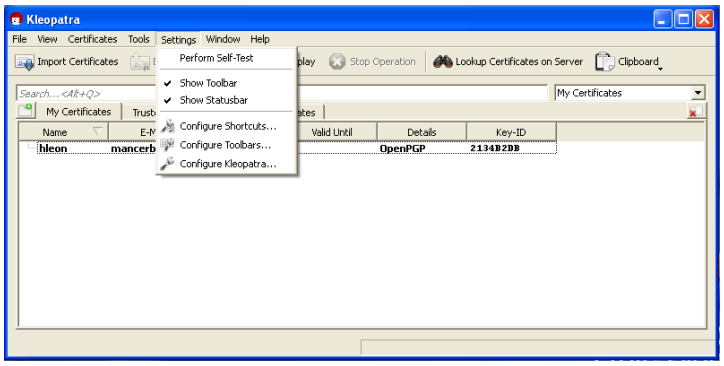


Fig.112. Proceso de almacenamiento de la llave pública desde el usuario (Departamentos de Ventas y Finanzas) al servidor Ubuntu Server Keys

2. Ahora se da click en el icono de la ventana "New" para ingresar la información siguiente correspondiente al servidor Ubuntu Server Keys:

   Scheme (modo de conexión al servidor Ubuntu Server Keys): hkp
   Server name (dirección IP del servidor Ubuntu Server Keys): 192.168.0.12
   Server Port (Puerto de comunicación del servidor Ubuntu Server Keys): 11371
   OpenPGP: Se selecciona esta opción

   A continuación se da click en el icono "Apply" y el icono "OK" para guardar la configuración asignada.

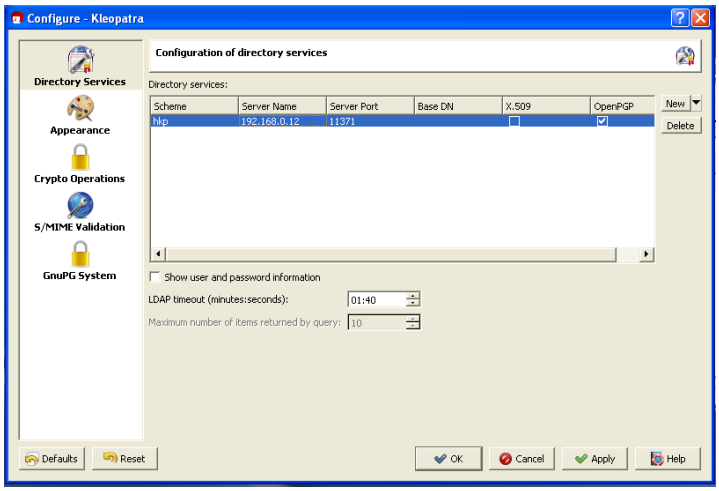


Fig.113. Proceso de almacenamiento de la llave pública desde el usuario (Departamentos de Ventas y Finanzas) al servidor Ubuntu Server Keys

3. Después se da click derecho con el mouse encima de la llave pública que aparece en la ventana del programa, y se selecciona la opción "Export certificates to server".

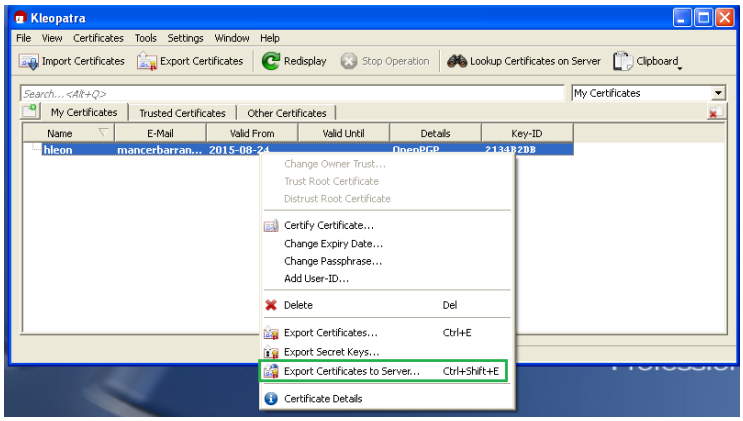


Fig.114. Proceso de almacenamiento de la llave pública desde el usuario (Departamentos de Ventas y Finanzas) al servidor Ubuntu Server Keys

4. El programa pedirá la confirmación del usuario del envió de la llave pública desde el sistema operativo Windows XP1 o Windows XP2 al servidor Ubuntu Server Keys, haciendo click en el icono "Continue".

Fig.115. Proceso de almacenamiento de la llave pública desde el usuario (Departamentos de Ventas y Finanzas) al servidor Ubuntu Server Keys

5. Por último el sistema generará una ventana donde confirmará que la llave pública ha sido almacenada correctamente en el servidor Ubuntu Server Keys.
   Ahora se da click en el icono "OK" para terminar el proceso.

Fig.116. Proceso de almacenamiento de la llave pública desde el usuario (Departamentos de Ventas y Finanzas) al servidor Ubuntu Server Keys

PROCESO DE ENCRIPTACIÓN Y ALMACENAMIENTO DE ARCHIVOS EN EL REPOSITORIO UBUNTU SERVER SSH (PARA USUARIOS WINDOWS XP1 y XP2)

Proceso de Encriptación:

Para el proceso de encriptación se debe tener en cuenta el mismo procedimiento realizado para los usuarios Linux (Departamento de Operaciones).

1. Se crea un archivo de cualquier tipo de formato para realizar el proceso de encriptación, para este caso se realizará el ejemplo con archivo de imagen (.jpg).

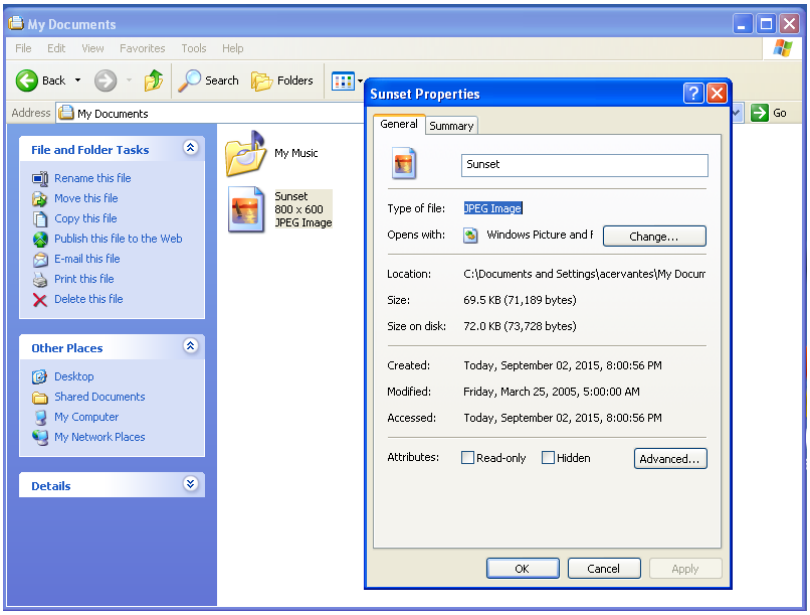


Fig.117. Proceso de encriptación de archivos mediante el uso de la llave pública del usuario Windows XP1 o XP2 que desea ver la información.

2. A continuación se descarga desde el servidor Ubuntu Server Keys la llave pública del usuario que desea ver la información para realizar el proceso de encriptación. Para ello es

necesario dar click en el icono “Lookup Certificates on Server” de la barra de herramientas del programa Kleopatra.

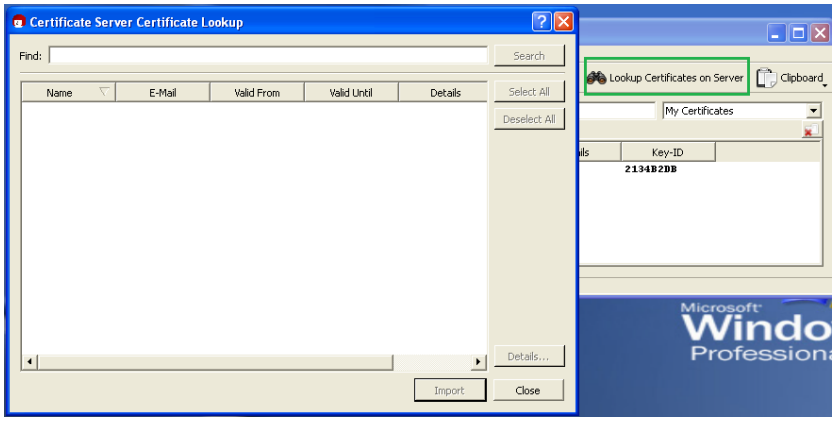


Fig.118. Proceso de encriptación de archivos mediante el uso de la llave pública del usuario Windows XP1 o XP2 que desea ver la información.

3. Ahora el sistema generara una ventana en la que se debe ingresar el número ID de la llave pública del usuario que desea ver la información, teniendo en cuenta la siguiente forma para su búsqueda y descarga.

0x(últimos 8 dígitos del número ID)

Para este caso se buscará y descargará la llave pública de un usuario del Departamento de Finanzas (mbarranco).

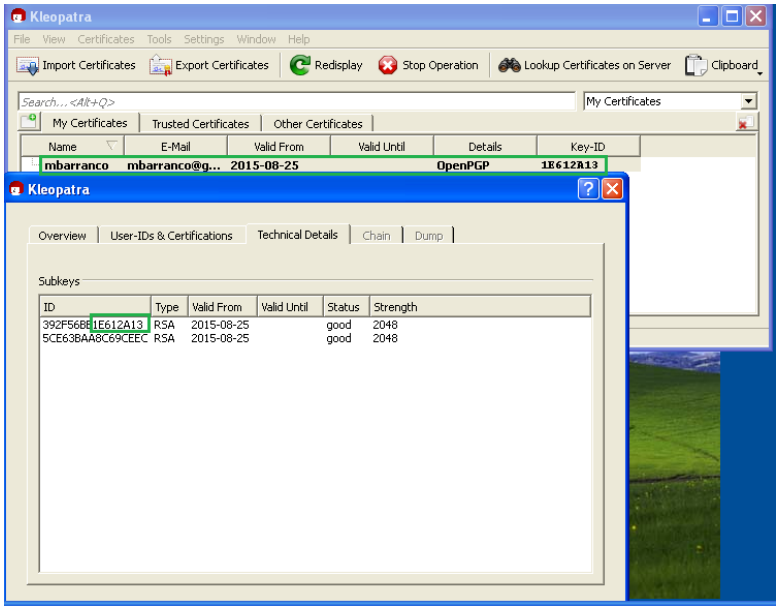


Fig.119. Proceso de encriptación de archivos mediante el uso de la llave pública del usuario Windows XP1 o XP2 que desea ver la información.

Ya ingresada la ID de la llave pública, se da click en el icono “Search” donde aparecerá una ventana emergente donde explicará los detalles que el usuario debe tener en cuenta para la búsqueda de la llave pública. Luego se da click en el icono “OK” para continuar con el proceso.

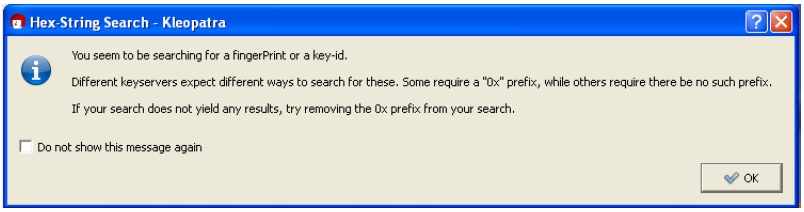


Fig.120. Proceso de encriptación de archivos mediante el uso de la llave pública del usuario Windows XP1 o XP2 que desea ver la información.

Después aparecerán en la ventana “Certificate Server Certificate Lookup” los detalles del usuario al cual corresponde el número ID para comprobar que el proceso se está realizando correctamente.

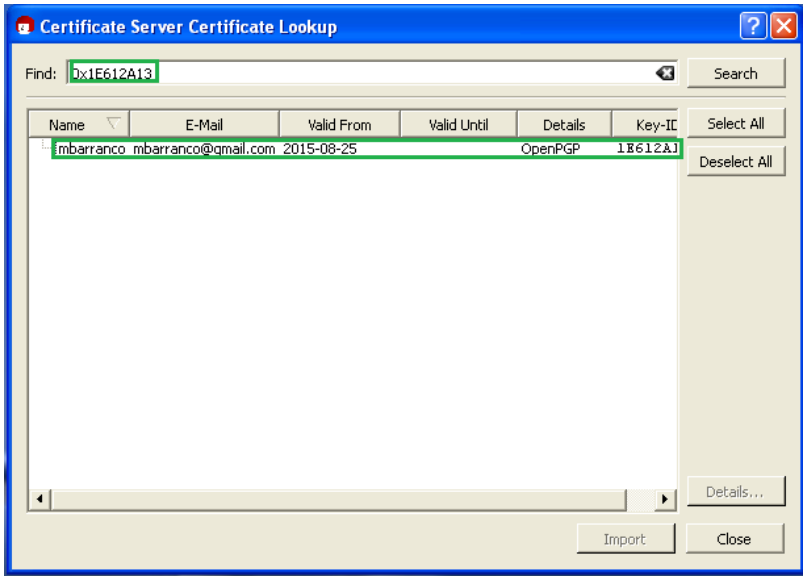


Fig.121. Proceso de encriptación de archivos mediante el uso de la llave pública del usuario Windows XP1 o XP2 que desea ver la información.

4. Para continuar con el proceso, se selecciona la llave pública descargada del usuario del Departamento de Finanzas y se da click en el icono “Import” para terminar el proceso de descarga de la llave pública. De lo anterior, se generará una ventana emergente donde se visualizará que el proceso ha sido realizado correctamente.

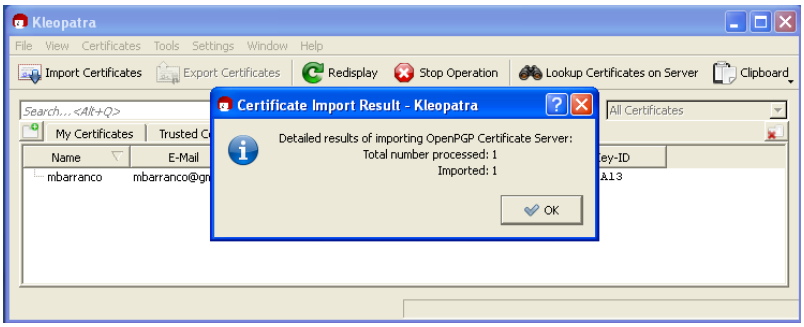


Fig.122. Proceso de encriptación de archivos mediante el uso de la llave pública del usuario Windows XP1 o XP2 que desea ver la información.

5. Teniendo en cuenta lo anterior, ahora se realizará el proceso de encriptación de manera sencilla. Primero se debe ir a la ubicación del archivo (Sunset.jpg), hacer click derecho con el mouse en el archivo y seleccionar las opciones “More GpgEX options” y “Encrypt”.

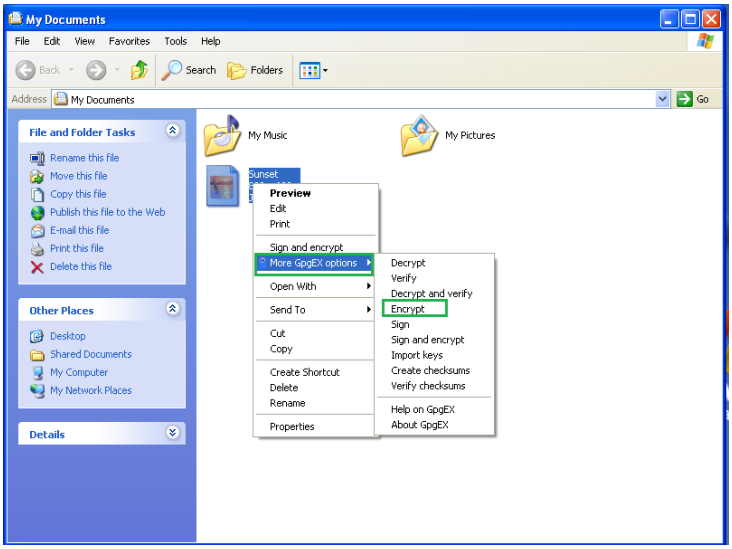


Fig.123. Proceso de encriptación de archivos mediante el uso de la llave pública del usuario Windows XP1 o XP2 que desea ver la información.

6. A continuación se abrirá una ventana emergente que corresponde al programa Kleopatra (“Sign/Encrypt Files”) donde aparecerá por defecto la opción de encriptar archivos (“Encrypt”) seleccionada por el programa automáticamente, al igual que la ubicación del archivo a encriptar. Luego se da click en el icono “Next” para continuar con el proceso.

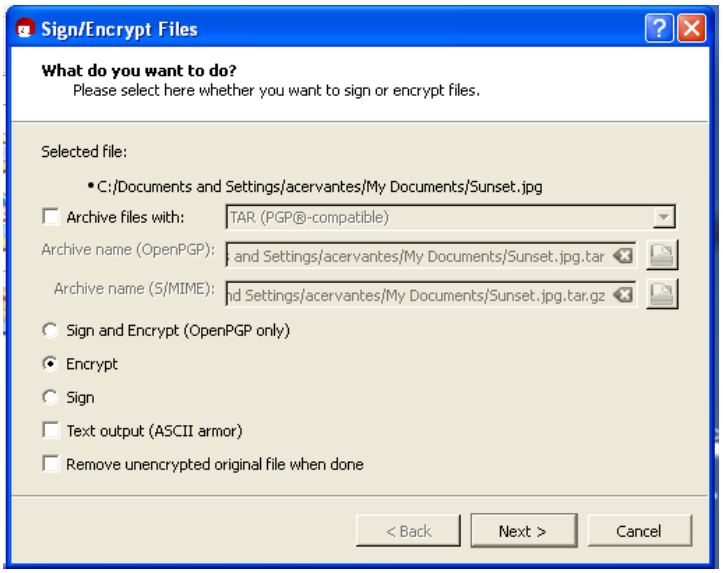


Fig.124. Proceso de encriptación de archivos mediante el uso de la llave pública del usuario Windows XP1 o XP2 que desea ver la información.

7. Después el programa preguntará al usuario con cuál de las llaves públicas se realizará el proceso de encriptación, para el caso del ejemplo se seleccionara el usuario del Departamento de Finanzas (mbarranco). Ahora se da click en el icono "Add" y en el icono "Encrypt" para continuar con el proceso.

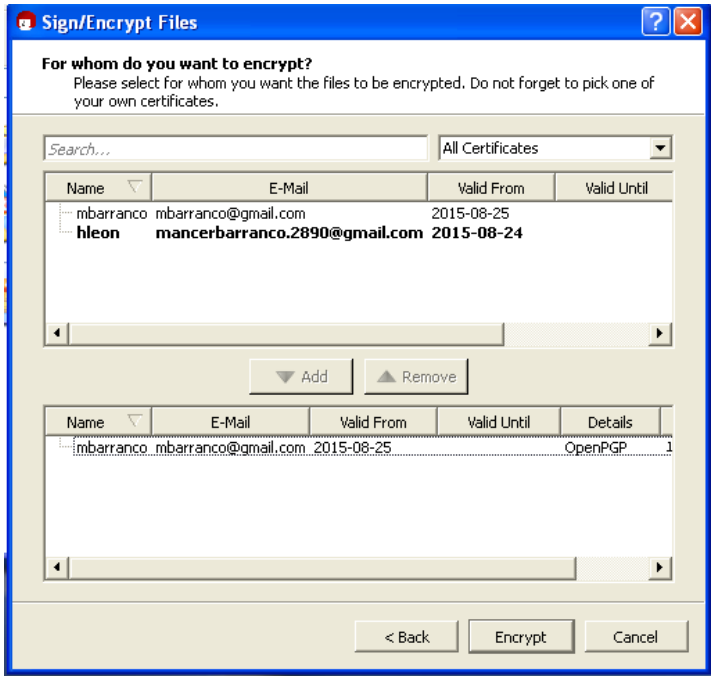


Fig.125. Proceso de encriptación de archivos mediante el uso de la llave pública del usuario Windows XP1 o XP2 que desea ver la información.

8. Ahora el programa arrojará una ventana emergente “Encrypt to self warning-Keopatra” donde le informa al usuario que una vez realice el proceso de encriptación no podrá des-encriptar el archivo, debido a que no tiene la llave privada del usuario con el que va a realizar el proceso de des-encriptación. Se da click en el icono “Continue” para seguir con el proceso.

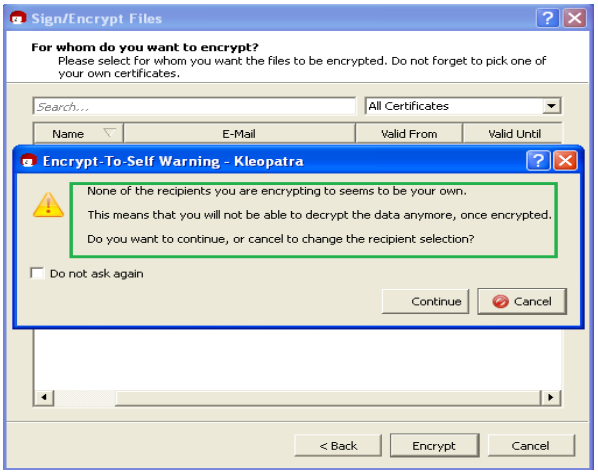


Fig.126. Proceso de encriptación de archivos mediante el uso de la llave pública del usuario Windows XP1 o XP2 que desea ver la información.

9. Luego aparecerá una ventana que le indica al usuario que el proceso de encriptación ha sido realizado correctamente.

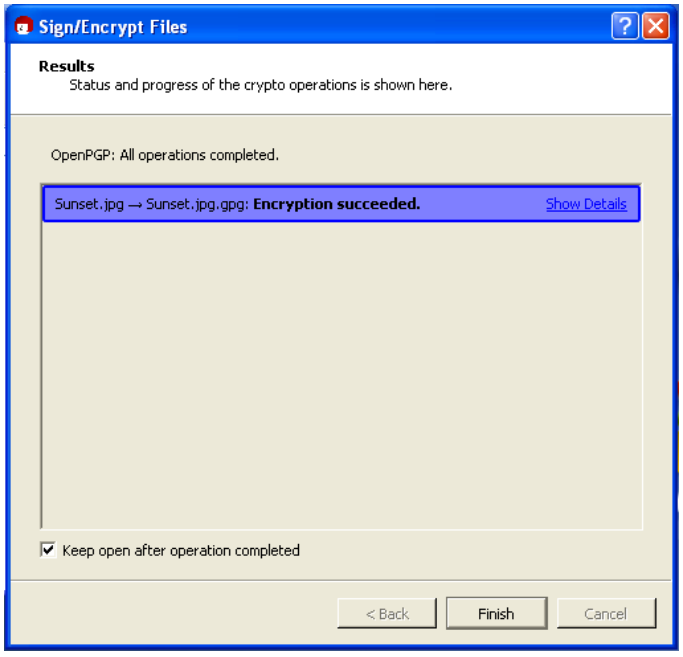


Fig.127. Proceso de encriptación de archivos mediante el uso de la llave pública del usuario Windows XP1 o XP2 que desea ver la información.

10. Por último, se genera el archivo encriptado (sunset.jpg.gpg) en la misma ubicación del archivo a encriptar tal como aparece en la imagen.

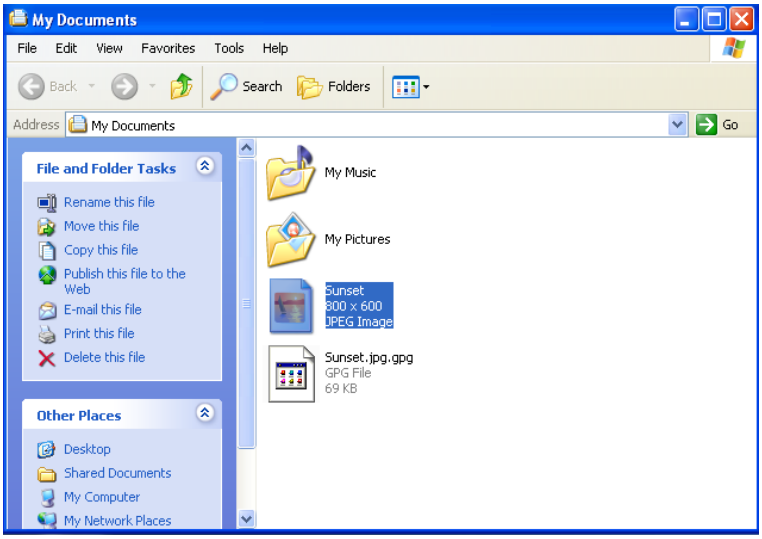


Fig.128. Proceso de encriptación de archivos mediante el uso de la llave pública del usuario Windows XP1 o XP2 que desea ver la información.

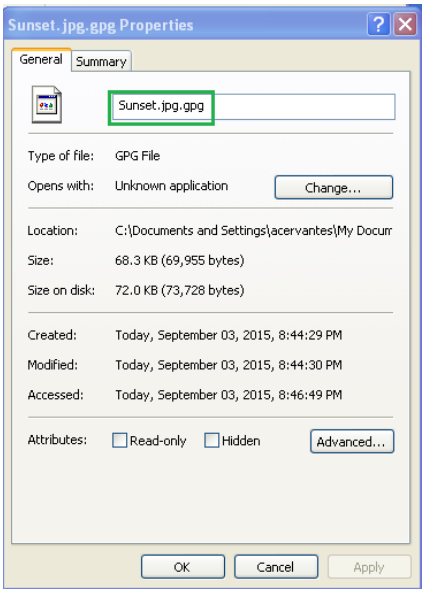


Fig.129. Proceso de encriptación de archivos mediante el uso de la llave pública del usuario Windows XP1 o XP2 que desea ver la información.

Para comprobar que el archivo generado es el encriptado, tan solo se trata de abrir con otros programas donde se verifica que no se puede observar la información verdadera.

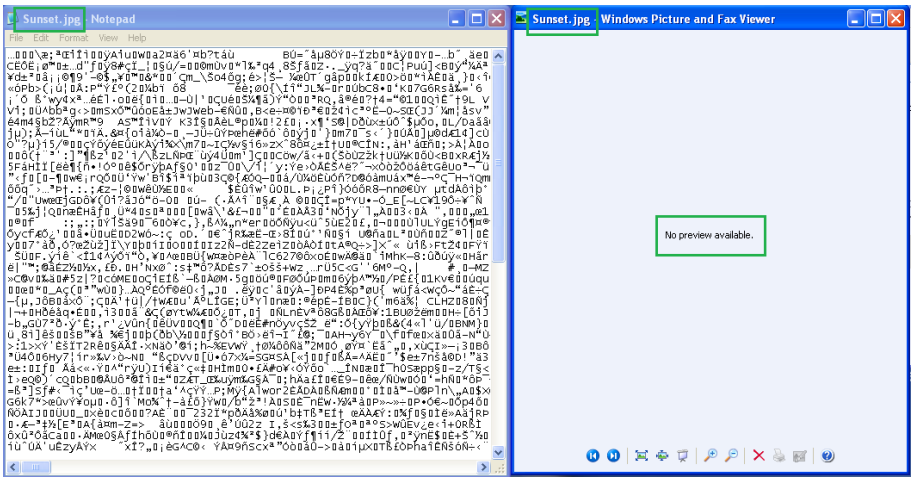


Fig.130. Proceso de encriptación de archivos mediante el uso de la llave pública del usuario Windows XP1 o XP2 que desea ver la información.

Proceso de almacenamiento de archivos en el repositorio Ubuntu Server SSH:

Teniendo el archivo encriptado (Sunset.jpg.gpg) ahora se realiza el proceso de almacenamiento del archivo en el repositorio Ubuntu Server SSH, con la ayuda del programa ejecutable (Psftp.exe) el cual es una herramienta para la transferencia de archivos de forma segura entre ordenadores utilizando la conexión SSH.

11. Primero se abre la consola de Windows (XP1 o XP2) CMD, en la que se ingresará a la ubicación del programa PSFTP.
    Para el caso del ejemplo, el programa se encontrará alojado en la ubicación:
    C:\Documents and Settings\mleon\Desktop\My Documents

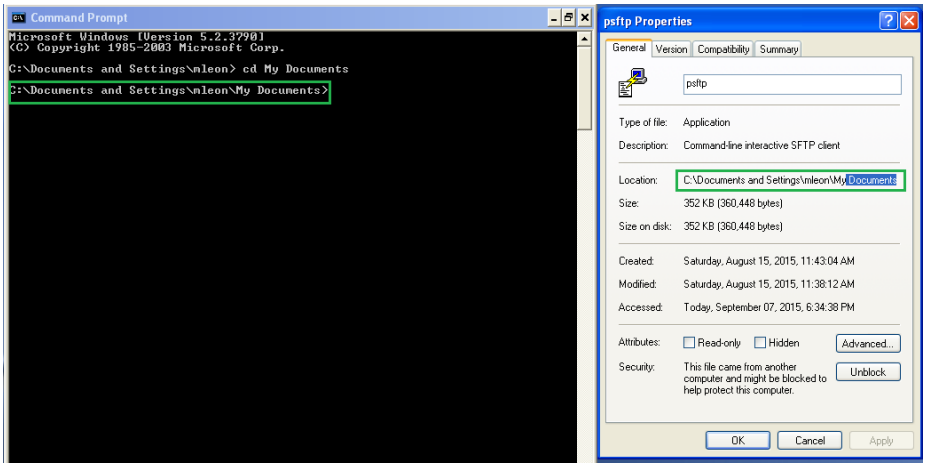


Fig.131. Proceso de almacenamiento de archivos desde el usuario Windows XP1 o XP2 al repositorio Ubuntu Server SSH

12. Ahora se digita el comando “DIR” para poder visualizar la información de la carpeta “My Documents” y así poder ejecutar por consola el programa PSFTP.
    Además de visualizar la ubicación del archivo encriptado “Sunset.jpg.gpg”.

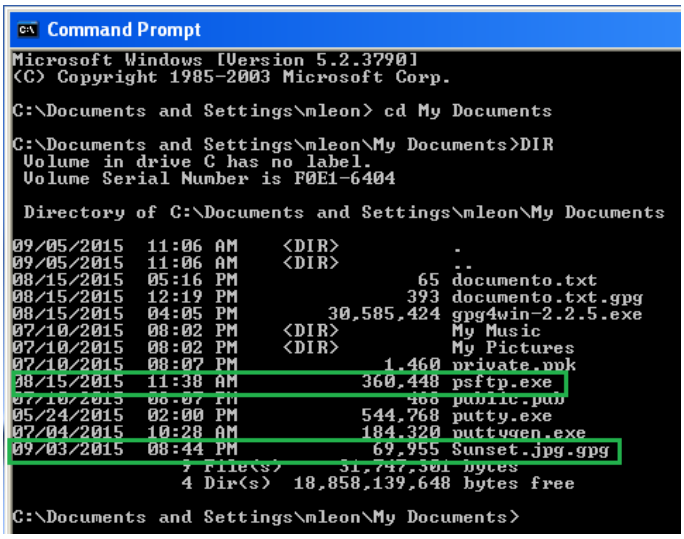


Fig.132. Proceso de almacenamiento de archivos desde el usuario Windows XP1 o XP2 al repositorio Ubuntu Server SSH

13. Después se digita el nombre del ejecutable del programa PSFTP “psftp.exe” para poder empezar el proceso de almacenamiento de archivos en el repositorio Ubuntu Server SSH.

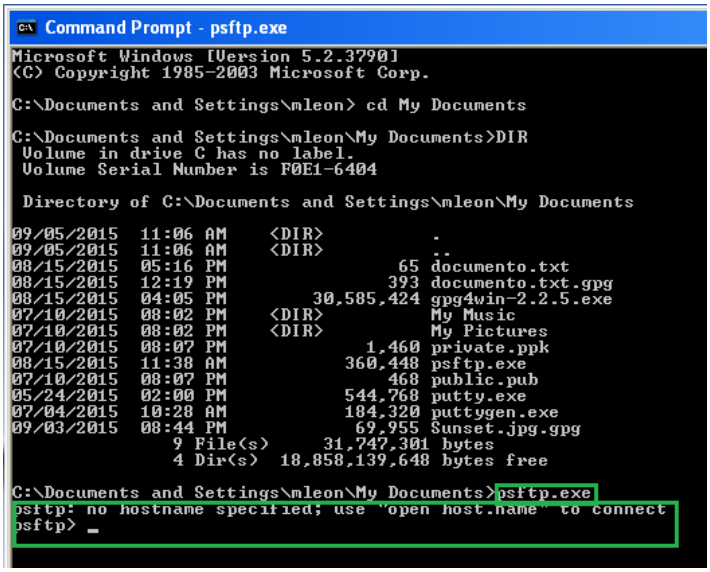


Fig.133. Proceso de almacenamiento de archivos desde el usuario Windows XP1 o XP2 al repositorio Ubuntu Server SSH

14. Luego se ingresa con el usuario del Departamento de Ventas o Finanzas "mleon" correspondiente, al repositorio Ubuntu Server SSH mediante el protocolo PSFTP usando el siguiente comando:

    Open (Usuario Windows XP1 o XP2)@(Dirección IP del repositorio Ubuntu Server SSH)

    Después el programa confirmará el usuario "mleon" y permitirá la transferencia de archivos desde el usuario Windows XP1 o XP2 al repositorio.

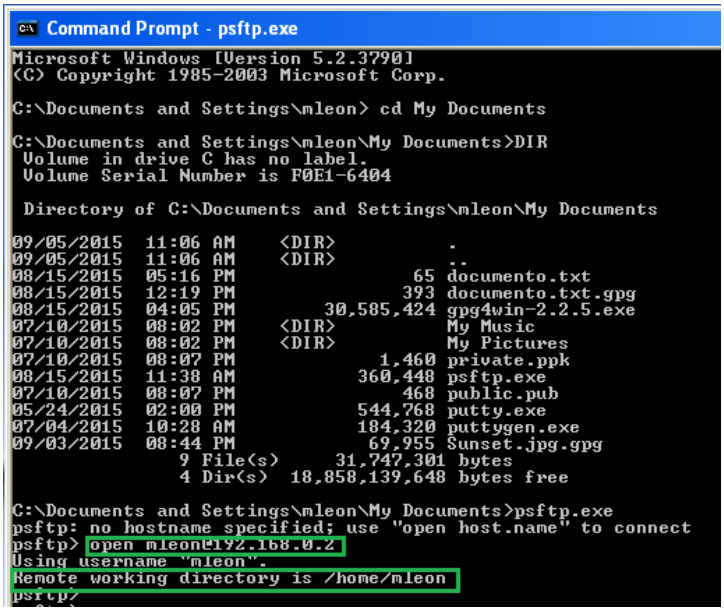


Fig.134. Proceso de almacenamiento de archivos desde el usuario Windows XP1 o XP2 al repositorio Ubuntu Server SSH

15. Una vez estando el usuario Windows XP1 o XP2 en el repositorio Ubuntu Server SSH, se ingresa a la ubicación de las carpetas o carpeta en la que se almacenará el archivo encriptado, mediante el siguiente comando:

    Cd /orange/(carpeta del Departamento de Ventas o Finanzas que se requiera)

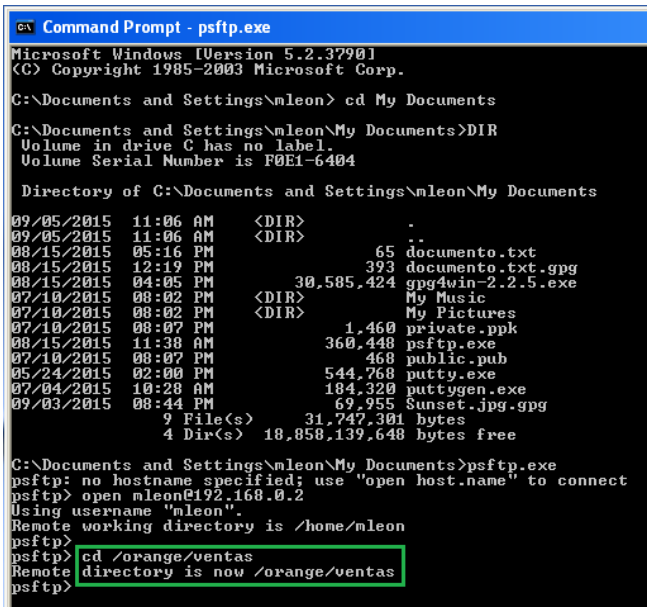


Fig.135. Proceso de almacenamiento de archivos desde el usuario Windows XP1 o XP2 al repositorio Ubuntu Server SSH

16. A continuación se almacena el archivo encriptado desde el usuario Windows XP1 o XP2 al repositorio Ubuntu Server SSH, mediante el siguiente comando:

Put (Ubicación del archivo encriptado (Sunset.jpg.gpg))

Fig.136. Proceso de almacenamiento de archivos desde el usuario Windows XP1 o XP2 al repositorio Ubuntu Server SSH

Como se observa en la imagen, el programa ilustra la transferencia segura de archivos desde el usuario del Departamento de Ventas "mleon" (local) al repositorio Ubuntu Server SSH (remote).

17. Por último se revisa en el repositorio Ubuntu Server SSH el archivo encriptado "Sunset.jpg.gpg" ubicado en la carpeta "Ventas".

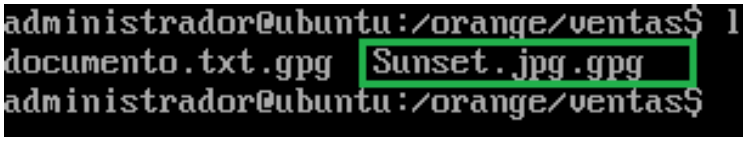


Fig.137. Proceso de almacenamiento de archivos desde el usuario Windows XP1 o XP2 al repositorio Ubuntu Server SSH

PROCESO DE DESCARGA Y DES-ENCRIPTACIÓN DE ARCHIVOS DEL REPOSITORIO UBUNTU SERVER SSH A LOS USUARIOS XP (DEPARTAMENTOS DE VENTAS Y FINANZAS)

Cabe aclarar que para desarrollar este proceso se debe tener presente el usuario que desea ver la información encriptada, ya que según el proceso de encriptación asimétrica sólo se puede des-encriptar la información mediante la llave privada del usuario.
Para el caso del ejemplo, el archivo "Sunset.jpg" fue encriptado con la llave pública del usuario "mbarranco" el cuál des-encriptará la información del archivo "Sunset.jpg.gpg" con la llave privada que sólo este usuario posee.

Proceso de descarga de archivos desde el repositorio Ubuntu Server SSH a los usuarios XP (Departamentos de Ventas y Finanzas):

1. Estando en el escritorio del usuario "mbaranco", se ingresará al ejecutable del programa PSFTP "psftp.exe" para poder empezar el proceso de descarga de archivos desde el repositorio Ubuntu Server SSH a usuario XP1 o XP2.

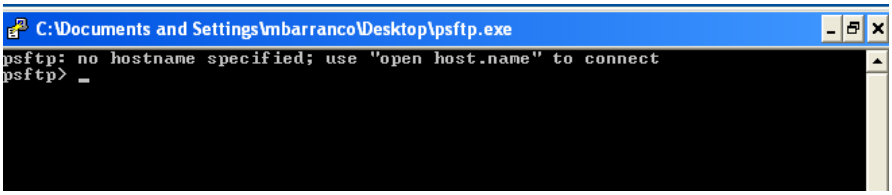


Fig.138. Proceso de descarga de archivos desde el repositorio Ubuntu Server SSH al usuario Windows XP1 o XP2

2. A continuación se ingresa al repositorio remotamente con el usuario "mbarranco", ingresando en la consola el siguiente comando:

Open (nombre del usuario del Departamento de Ventas o Finanzas)@(dirección IP del repositorio Ubuntu Server SSH)

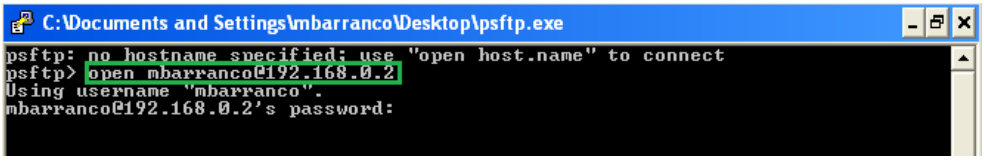


Fig.139. Proceso de descarga de archivos desde el repositorio Ubuntu Server SSH al usuario Windows XP1 o XP2

Se ingresa la contraseña de acceso correspondiente a "mbarranco".

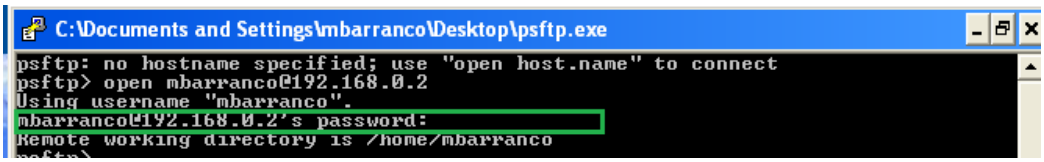


Fig.140. Proceso de descarga de archivos desde el repositorio Ubuntu Server SSH al usuario Windows XP1 o XP2

3. Luego el sistema indicará la ubicación del usuario en el repositorio Ubuntu Server SSH (/home/mbarranco).

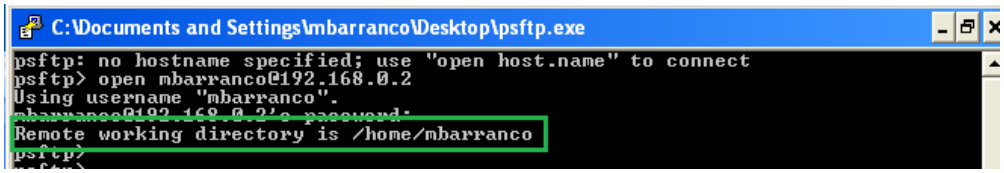


Fig.141. Proceso de descarga de archivos desde el repositorio Ubuntu Server SSH al usuario Windows XP1 o XP2

4. Ahora se descarga el archivo encriptado "Sunset.jpg.gpg", desde esa ubicación ingresando a la consola el siguiente comando:

   Get (ubicación del archivo encriptado en el repositorio Ubuntu Server SSH)

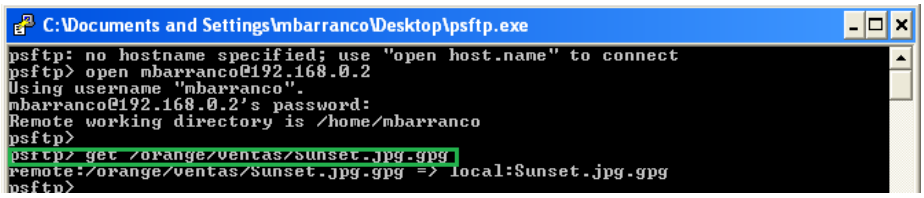


Fig.142. Proceso de descarga de archivos desde el repositorio Ubuntu Server SSH al usuario Windows XP1 o XP2

El programa ilustrará la ruta desde donde se descarga el archivo (repositorio Ubuntu Server SSH) hacia la ubicación local (Usuario Windows XP1 o XP2). Para este caso no se indicó ninguna ruta local del usuario "mbarranco", por tal motivo el programa descarga el programa en el escritorio como se indica en la imagen:

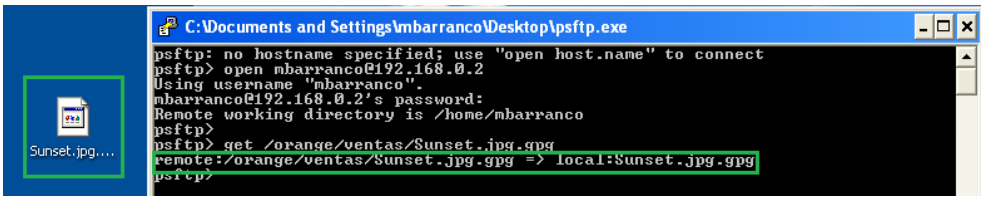


Fig.143. Proceso de descarga de archivos desde el repositorio Ubuntu Server SSH al usuario Windows XP1 o XP2

5. Por último, se verifica que el archivo descargado en el escritorio del usuario “mbarranco” corresponda al indicado.

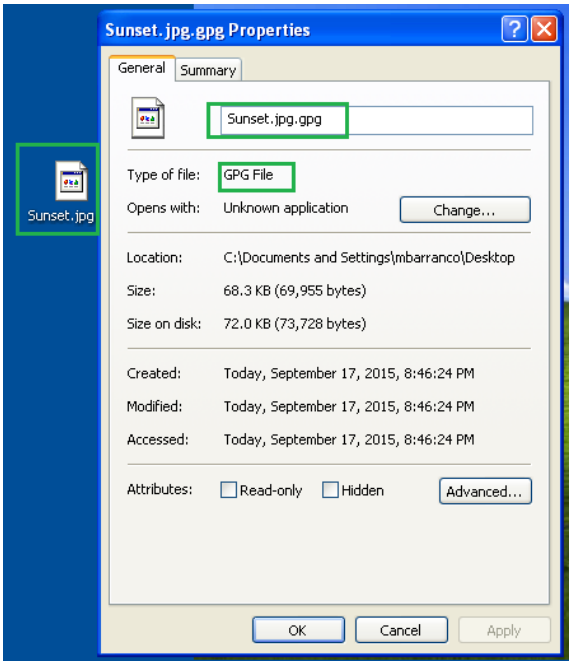


Fig.144. Proceso de descarga de archivos desde el repositorio Ubuntu Server SSH al usuario Windows XP1 o XP2

Proceso de des-encriptación de archivos del repositorio Ubuntu Server SSH a los usuarios XP1 o XP2 (Departamentos de Ventas y Finanzas):

Para el proceso de des-encriptación es necesario tener la llave privada del usuario que desea ver la información, para este caso el usuario del departamento de finanzas “mbarranco”.
A continuación se describe el proceso.

1. Teniendo el archivo encriptado “Sunset.jpg.gpg” descargado del repositorio Ubuntu Server SSH, se da click derecho con el mouse en el archivo y se elige la opción “MoreGpgEX options” y se selecciona el icono “Decrypt” para empezar el proceso.

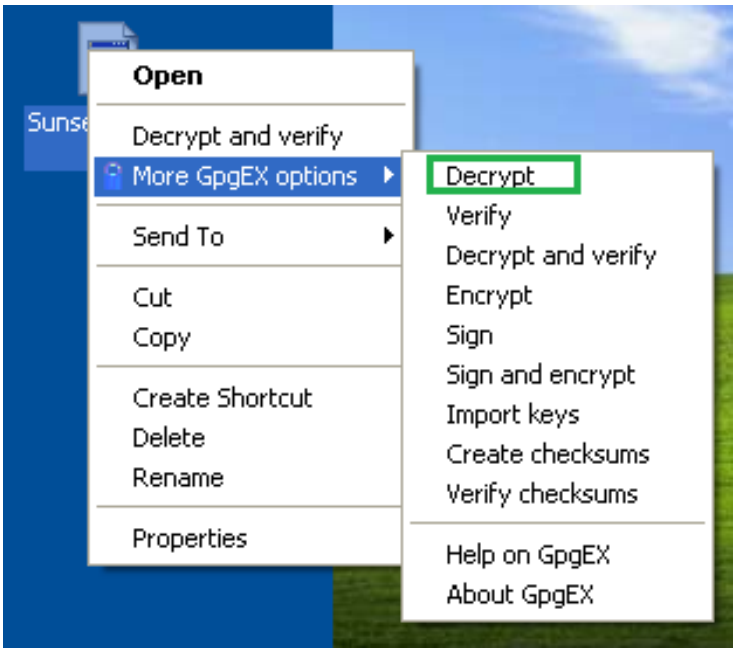


Fig.145. Proceso de des-encriptación de archivos en el equipo del usuario Windows XP1 o XP2 (Departamentos de Ventas y Finanzas)

2. A continuación se abrirá una ventana emergente proveniente del software de encriptación y des-encriptación de archivos Kleopatra, llamada "Decrypt/Verify Files" donde se hará click en el icono "Decrypt/Verify" para continuar con el proceso.

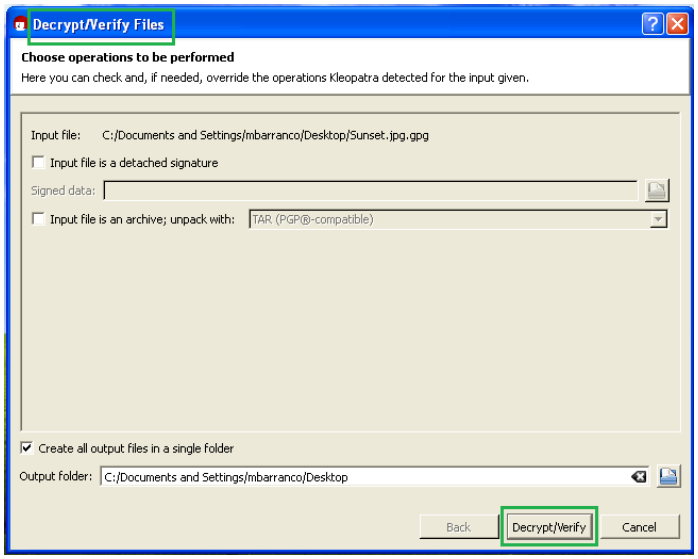


Fig.146. Proceso de des-encriptación de archivos en el equipo del usuario Windows XP1 o XP2 (Departamentos de Ventas y Finanzas)

3. Luego el software generará otra ventana emergente llamada "pinentry" donde pedirá ingresar la contraseña (Passphrase) para desbloquear la llave privada del usuario que desea

ver la información “mbarranco” y así continuar con el proceso de des-encriptación del archivo.

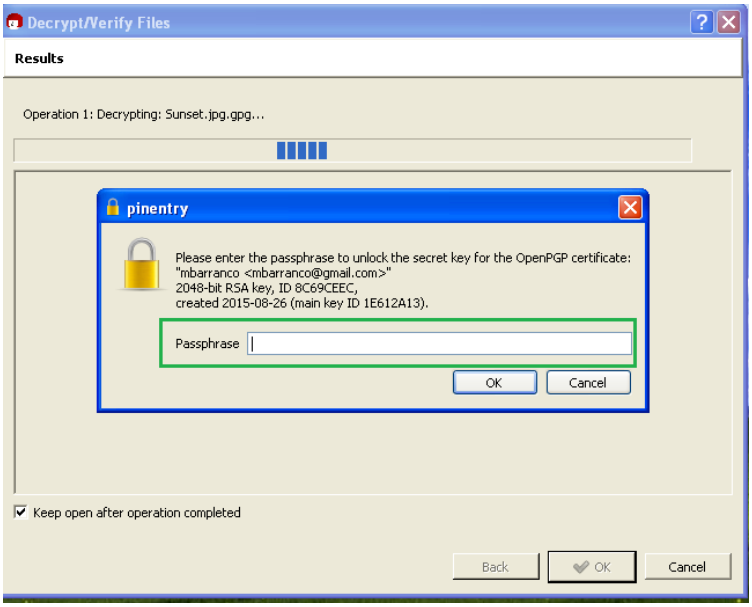


Fig.147. Proceso de des-encriptación de archivos en el equipo del usuario Windows XP1 o XP2 (Departamentos de Ventas y Finanzas)

4. Cuando el proceso se ha culminado, el mismo software generará un aviso en el cual le confirma al usuario que el proceso ha terminado. Después se da click en el icono “OK” para terminar el proceso.
   Como se puede apreciar en la imagen, se ha des-encriptado el archivo tipo imagen (JPG) “Sunset.jpg”.

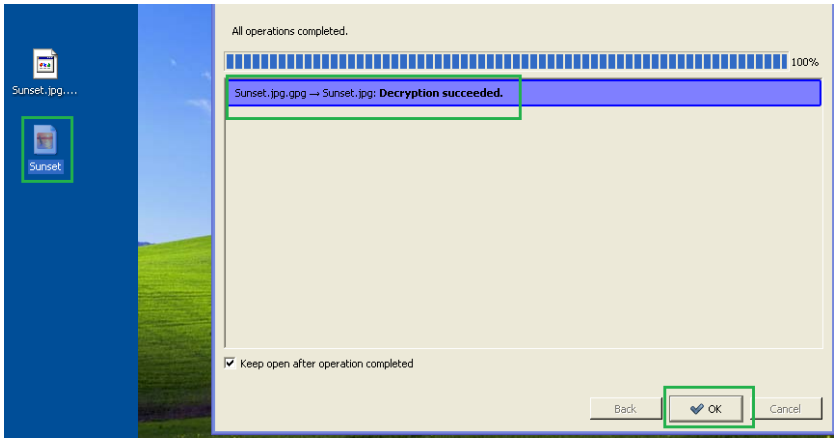


Fig.148. Proceso de des-encriptación de archivos en el equipo del usuario Windows XP1 o XP2 (Departamentos de Ventas y Finanzas)

5. Por último se comprueba que el archivo des-encriptado sea el que el usuario "mbarranco" requiere ver su información, haciendo click derecho con el mouse en el archivo y seleccionando el icono "Properties" tal como se ve en la imagen.

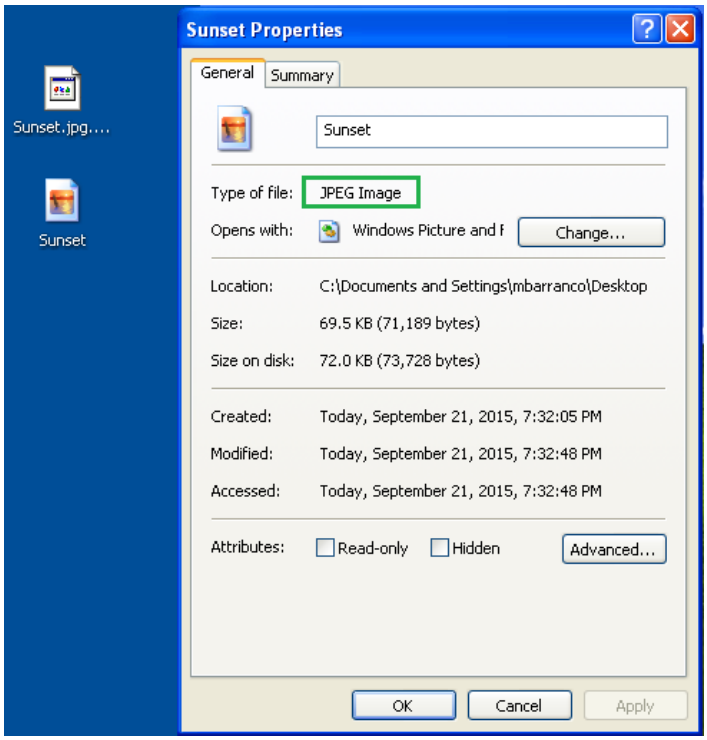


Fig.149. Proceso de des-encriptación de archivos en el equipo del usuario Windows XP1 o XP2 (Departamentos de Ventas y Finanzas)

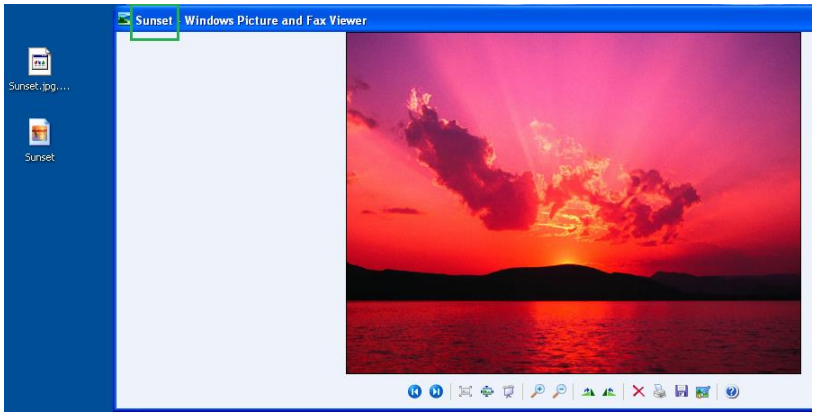


Fig.150. Proceso de des-encriptación de archivos en el equipo del usuario Windows XP1 o XP2 (Departamentos de Ventas y Finanzas)

ENJAULADO DE USUARIOS EN EL REPOSITORIO UBUNTU SERVER SSH

El proceso de enjaulado de usuarios es fundamental para la implementación del repositorio con seguridad, ya que garantiza la privacidad y exclusividad de las carpetas entre los Departamentos de la empresa.

1. Primero se debe buscar el archivo de configuración del repositorio Ubuntu Server SSH (sshd_config), en la siguiente ubicación:

   Cd /etc/ssh

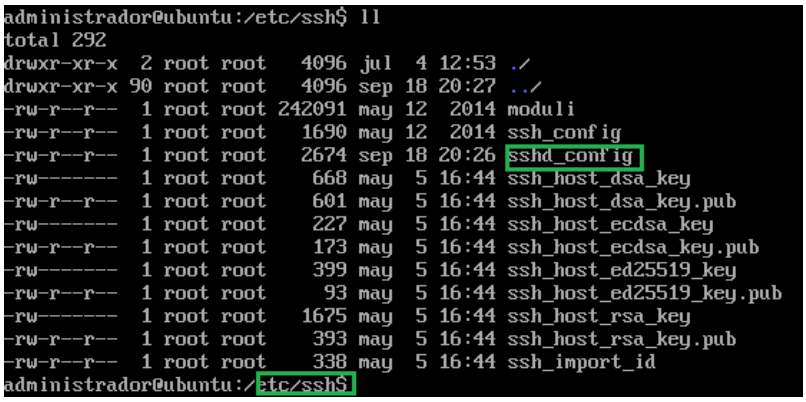


Fig.151. Proceso de enjaulado de usuarios en el repositorio Ubuntu Server SSH

2. Ahora se debe ingresar al archivo mediante el editor de texto “nano” para realizar los cambios para el enjaulado:

   Sudo nano sshd_config

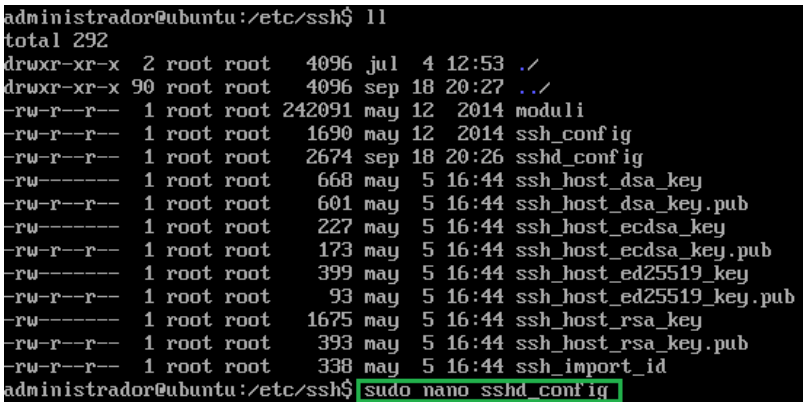


Fig.152. Proceso de enjaulado de usuarios en el repositorio Ubuntu Server SSH

3. Una vez se ingrese al archivo “sshd_config” en la última parte del archivo se ingresan los siguientes comandos para generar los permisos de ingreso de los usuarios a las carpetas respectivas:

   Subsystem sftp internal-sftp

Match group (nombre del grupo del departamento)
ChrootDirectory (ubicación de la carpeta del departamento)
ForceCommand internal-sftp
AllowTCPForwarding no
X11Forwarding no

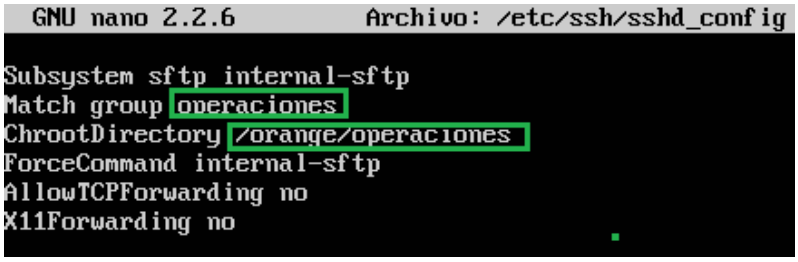


Fig.153. Proceso de enjaulado de usuarios en el repositorio Ubuntu Server SSH

4. A continuación se almacena la configuración realizada presionando las teclas "Ctrl+o" y luego las teclas "Ctrl+x" para salir del editor de texto nano.

Fig.154. Proceso de enjaulado de usuarios en el repositorio Ubuntu Server SSH

5. Una vez se haya salido del editor de texto nano, queda reiniciar el repositorio Ubuntu Server SSH para que el sistema tome la nueva configuración, mediante el siguiente comando:

Sudo service ssh restart

6. Después se deben dar los permisos de escritura, lectura y ejecución de los archivos al propietario de la carpeta (Departamento de operaciones, ventas o finanzas), mediante el siguiente comando:

Sudo chmod 755 (ubicación de la carpeta del departamento)

Fig.155. Proceso de enjaulado de usuarios en el repositorio Ubuntu Server SSH

7. Por último queda verificar que el proceso sea realizado correctamente, ingresando mediante el protocolo sftp al repositorio Ubuntu Server SSH desde el departamento al cuál se le haya asignado la configuración de enjaulado, por medio del siguiente comando:

Sftp phernandez@(dirección IP del servidor)

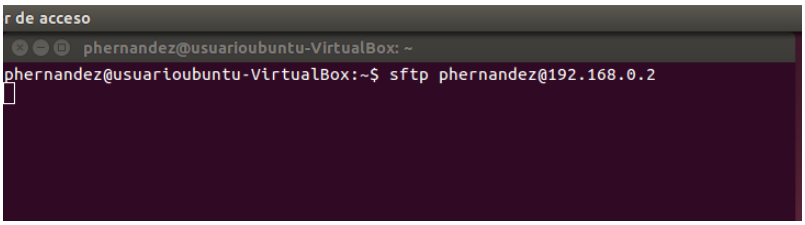


Fig.156. Proceso de enjaulado de usuarios en el repositorio Ubuntu Server SSH

El sistema pedirá ingresar la contraseña (clave privada) propia de cada usuario para dar ingreso al repositorio Ubuntu Server SSH:

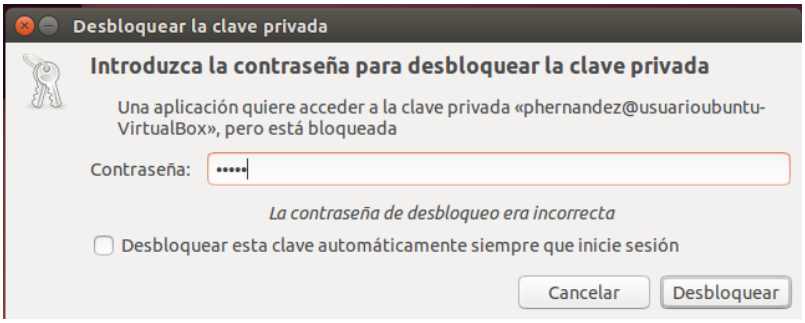


Fig.157. Proceso de enjaulado de usuarios en el repositorio Ubuntu Server SSH

Luego el sistema ingresará al repositorio de forma segura mediante el protocolo sftp, donde se digita el siguiente comando para verificar la ubicación en la que está el usuario del departamento de operaciones, ventas o finanzas:

Ls

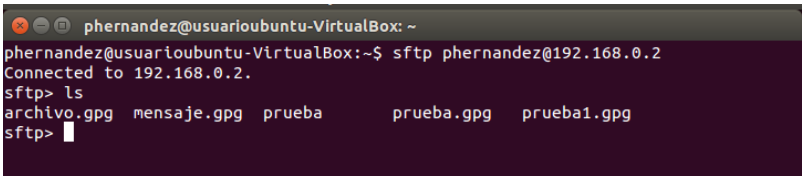


Fig.158. Proceso de enjaulado de usuarios en el repositorio Ubuntu Server SSH

El usuario (phernandez) del Departamento de Operaciones tiene acceso a los archivos de la carpeta Operaciones del repositorio Ubuntu Server SSH.
Para comprobarlo mejor, se debe ingresar al repositorio Ubuntu Server SSH y verificar en la carpeta Operaciones si los archivos corresponden a los que se visualizan en la imagen anterior.

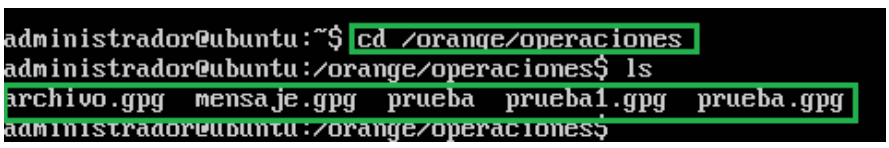


Fig.159. Proceso de enjaulado de usuarios en el repositorio Ubuntu Server SSH

Como se visualiza, tanto en el repositorio Ubuntu Server SSH como en el usuario (phernandez) del departamento de Operaciones, los archivos corresponden a la carpeta Operaciones.

INSTALACIÒN DE FIREWALL (IPTABLES)

Es importante tener presente en la implementación del repositorio con seguridad la instalación del firewall (IPTABLES), ya que garantiza la seguridad de la información de los usuarios de los diferentes departamentos de la empresa en cuanto a la transferencia de archivos, mediante la asignación de reglas permitiendo el filtrado del tráfico de red.

1. Primero se debe iniciar el servicio IPTables mediante el siguiente comando:

   Sudo service iptables start

2. Una vez iniciado el servicio Firewall, se asignan las reglas para permitir la transferencia de información por el protocolo SSH (puerto 22), mediante el siguiente comando:

Sudo iptables –A(permite agregar una regla) INPUT –p(permite aplicar la regla a un protocolo) tcp –deport(selecciona o excluye puertos de un determinado puerto de destino) ssh –j ACCEPT

Fig.160 Proceso de Instalación de Firewall en el repositorio Ubuntu Server SSH

3. A continuación se verifica que las reglas aplicadas a la transferencia de archivos por el protocolo SSH (puerto 22) hayan sido asignadas correctamente, mediante el siguiente comando:

   Sudo iptables –L(muestra las reglas que han sido asignadas)

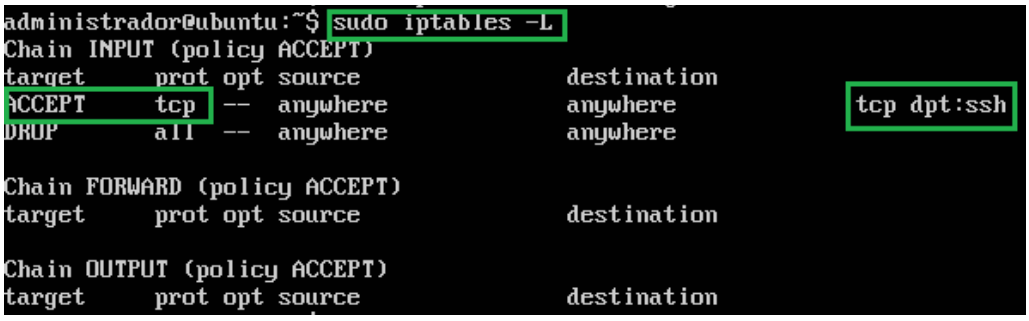


Fig.161. Proceso de Instalación de Firewall en el repositorio Ubuntu Server SSH

Como se puede observar en la imagen, se asignaron las reglas del firewall al protocolo SSH.

4. Por último se deben guardar las reglas establecidas, ya que al reiniciar el repositorio Ubuntu Server SSH perderá la configuración de las reglas asignadas. Se utiliza el siguiente comando para realizar el proceso de guardado de la configuración del firewall en un archivo (.fw) en el repositorio:

   Sudo iptables-save > /home/administrador/configuración/(nombre del archivo).fw

```
administrador@ubuntu:~$ sudo iptables-save > /home/administrador/configuracion/f
irew.fw_
```

Fig.162. Proceso de Instalación de Firewall en el repositorio Ubuntu Server SSH

A.5 Tabla de contraseñas de los usuarios (Departamentos de Operaciones, Ventas y Finanzas)

DEPARTAMENTO	SISTEMA OPERATIVO	USUARIO	CONTRASEÑA
OPERACIONES	LINUX	phernandez	colombia1
		caponte	colombia1
		apinillos	colombia2
VENTAS	WINDOWS XP1	mleon	colombia3
		hleon	colombia3
		fbernal	colombia5
FINANZAS	WINDOWS XP2	fsanchez	colombia4
		mbarranco	colombia4
		gleon	colombia5

A.6 Tabla de ID´s de llaves públicas y privadas de los usuarios (Departamentos de Operaciones, Ventas y Finanzas)

DEPARTAMENTO	SISTEMA OPERATIVO	USUARIO	ID LLAVE PUBLICA	ID LLAVE PRIVADA
OPERACIONES	LINUX	phernandez	A2FE2D311963193F	2C52F7EA3261318F
		caponte	BFD16A6282260B97	45F715B9479B61B6
		apinillos	5BBFB7A68D859F2D	9EA3A0218D945C94
VENTAS	WINDOWS XP1	mleon	72EF57E72904C1C3	2C9269BBA0CFD194
		hleon	0804C3292134B2DB	B004B64FD8759E40
		fbernal	41C4024223058101	B82CB2720F9EFB0D
FINANZAS	WINDOWS XP2	fsanchez	CEC834114C1076AE	C6563EB07E44DA56
		mbarranco	392F56BB1E612A13	5CE63BAA8C69CEEC
		gleon	E3AB17BA0EBD0FE0	98A545F8FB5D5456

A.7 Tabla de tiempos de encriptación de archivos (Windows XP Vs. Linux)

WINDOWS XP	LINUX
Archivo Texto: 30 Segundos	Archivo Texto: 60 Segundos
Archivo Imagen: 30 Segundos	Archivo Imagen: 60 Segundos

A.8 Tabla de tiempos de des-encriptación de archivos (Windows XP Vs. Linux)

WINDOWS XP	LINUX
Archivo Texto: 30 Segundos	Archivo Texto: 60 Segundos
Archivo Imagen: 30 Segundos	Archivo Imagen: 80 Segundos