Tipo de artículo: Artículo original

Seguridad en Sistemas Distribuidos caso proyecto FCI TEMONET de la Universidad de Guayaquil

Security in Distributed Systems case FCI TEMONET project of the University of Guayaquil

Jenny Arízaga-Gamboa[1*], **https://orcid.org/0000-0002-2098-9077**
Eduardo Alvarado-Unamuno[2], **https://orcid.org/0000-0001-6145-7926**
Jorge Chicala- Arroyave [3], **https://orcid.org/0000-0001-9630-2377**

[1] Universidad de Guayaquil, Ecuador. E-Mail: jenny.arizagag@ug.edu.ec
[2] Universidad de Guayaquil, Ecuador. E-Mail: eduardo.alvaradou@ug.edu.ec
[3] Universidad de Guayaquil, Ecuador. E-Mail: jorge.chicalaa@ug.edu.ec

*** Autor para correspondencia:** jenny.arizagag@ug.edu.ec

Resumen

En el presente trabajo se realiza un estudio en Seguridad de Sistemas Distribuidos, en el que señala las diversas características principales que implica la seguridad en la red, además incluyendo los desafíos principales que son piezas fundamentales que actuarán como barreras y procedimientos que resguardan el acceso a los datos y sólo permite acceder a las personas autorizadas para realizar dichas tareas. El estudio se aplica como soporte al trabajo de investigación del Proyecto FCI denominado TEMONET.

Palabras clave: Sistemas, Distribuidos, Cifrado, Seguridad, Software, Hardware.

Abstract

In this paper, a study on Distributed Systems Security is carried out, in which it indicates the various main characteristics that network security implies, as well as including the main challenges that are fundamental pieces that will act as barriers and procedures that protect access to the data and only allows access to people authorized to perform these tasks. The study is applied as a support to the research work of the FCI Project called TEMONET.

Keywords: *Systems, Distributed, Encryption, Security, Software, Hardware.*

Recibido: 22/12/2020
Aceptado: 18/03/2021

Introducción

En la actualidad la seguridad tiene un rol fundamental y primordial que permite proteger la información o datos de los clientes, es decir, es la técnica que restringe a tiempo el acceso a la información a personas no autorizado

que tiene la intención de obtener beneficio de la información almacenada. La Seguridad en Sistemas Distribuidos son recursos de computación físicamente interconectados a través de una red y con capacidad de coordinar con el fin de realizar una tarea, que tiene como objetivo la función de cliente servidor para realizar la comunicación, es decir, el cliente es la máquina que requiere de un servicio y el servidor es la máquina que va a proporcionar dicho servicio solicitado.

Sus principales pilares fundamentales son confidencialidad que se basa en proteger la información donde solo acceden personal autorizado, integridad se refiere a la entrega de información sin alteración alguna y disponibilidad al acceso a la información cuando se necesite. Un sistema distribuido es un método que contiene equipos de manera independiente que trabajan de modo transparente donde los usuarios observan el manejo del sistema operativo que se proyectan en diferentes CPU que permite tener varios procesadores con almacenamiento que se encuentran conectado a través de una red.

El objetivo principal de los sistemas distribuidos es disipar tanto el almacenamiento de la información como el procesamiento que contienen los dispositivos como son hardware y software que se encuentren conectado a través de la red y que permite crear comunicación, mediante un protocolo que es elegido por un esquema de modo cliente-servidor (López Espinoza, 2012).

Elementos de los Sistemas Distribuidos

Un sistema distribuido es el que se caracteriza por su transparencia que se aplica en todo su funcionamiento hasta el final de cualquier proceso que exista en el sistema donde se posee los elementos de trasparencia como:

- Transparencia en el acceso: La capacidad que tienen para encontrar recursos.
- Transparencia en respuestas: La capacidad que tienen para incrementar la confiabilidad del sistema.
- Transparencia en ubicación: La capacidad que tienen para ubicar la localización geográfica.
- Transparencia en concurrencias: La capacidad que tienen para trabajar al mismo tiempo los usuarios con las operaciones.
- Transparencia en fallas: La capacidad que tienen para que no se presente ningún error y seguir al margen.
- Transparencia en migración: La capacidad que tienen para poder realizar cambios donde no exista error y no afecte a los usuarios.
- Transparencia en rendimiento: La capacidad que tienen para poder ser reconfigurado sin ningún error, poder crecer y mejor su funcionamiento.
- Transparencia en escalabilidad: La capacidad que tienen para expandir su proceso donde se pueda aumentar o quitar dispositivos y permitan acoplarse al nuevo sistema.

- Transparencia: Es el que permite aplicar al usuario final en el momento que puede tener permiso en las aplicaciones que poseen en cualquier dispositivo que se encuentran conectadas en la red.

Materiales y métodos

En el transcurso de los años el tema seguridad se ha vuelto un tema importante que se debe analizar con detalles ya que sistemáticamente ocurre un sin número de violaciones con los datos que se guardan en un sistema. Teniendo en cuenta que no existe una técnica segura, pero que, si es posible resguardar la información, como por ejemplo seguir las reglas de cómo implementar una contraseña segura para que los atacantes no puedan invadir la privacidad (Carretero Pérez et al., 2001).

La seguridad de los sistemas es una técnica que permite proteger la información, datos o recursos de los clientes donde tienen como objetivo garantizar la seguridad o prevenir de todo peligro que este a su alcance para que dichos datos se encuentren de manera fiable. La seguridad es un proceso de prevenir o detectar a tiempo el uso de personas no autorizado que tiene la intención de obtener beneficio de la información almacenada (Carretero Pérez et al., 2001). Existen tres desafíos principales para proteger los datos (Ver Figura 1):

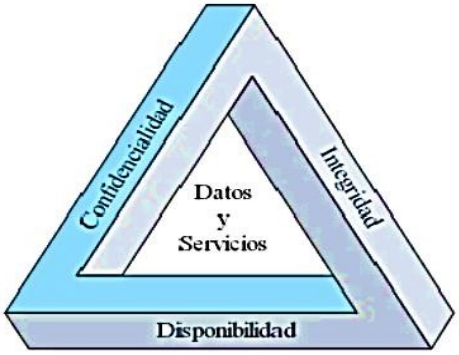

Figura 1. Pilares seguridad.

1. Confidencialidad o privacidad: Tiene como prioridad resguardar la información donde solo tengan acceso por usuarios que estén capacitados y solo para ellos se encuentre disponible (Areitio Bertolín, 2008).
2. Integridad: Tiene como tarea que dicha información se encuentre intacto y si se realiza un cambio solo puede ser posible por el personal que esté autorizado y sea detalle en la base de datos el cambio que realizo (Estupiñan et al., 2013).
3. Disponibilidad u operatividad: Es la capacidad de que dicha información siempre este en modo disponible para su uso y solo esté al alcance por usuarios autorizados, donde dichos datos deben estar

correctamente almacenados con hardware y software que deben estar trabajando perfectamente (Figueroa-Suárez et al., 2018).

Componentes de seguridad

Los tres componentes importantes que se deben tener presente para proteger a los sistemas informáticos son los datos, software y la parte del hardware (Solarte et al., 2015)

- Datos: Es el conjunto de información lógica que trabajan de la mano con la parte de hardware y software.
- Software: Es el conjunto de programas lógicos que trabaja de la mano con la parte de hardware para que funcione el sistema operativo.
- Hardware: Son todos los componentes físicos que utiliza una computadora o un sistema informático (Pérez Rueda, 2017).

Amenazas de seguridad

- Interrupción: Cuando un objeto del sistema se pierde puede suceder que pase a estado de no disponible.
- Interceptación: Cuando los usuario acceden a información no autorizada.
- Modificación: Cuando personas no autorizadas realizan cambios y no presentan los registros en la base de datos (Villacís & Morocho, 2017).

Tipos de seguridad

- **Seguridad física**: Es la que se encarga de prevenir y detectar a tiempo cuando se presenta una amenaza para que no cause anomalías en el sistema donde este tipo de seguridad se encarga de brindar seguridad a los sistemas, trata de poner barreras físicas y procesos de control para estar prevenidos cuando se presente una amenaza (Vera & Vera, 2017).
- **Seguridad lógica:** Tiene como tarea proteger la información que se encuentra dentro de su área de trabajo donde implementa protocolos de seguridad y técnicas para prevenir la divulgación de dicha información donde solo pueden acceder personas autorizadas. Tiene como tarea realizar:
  - Restringir el acceso a los programas y archivos.
  - El uso de los datos, archivos con el proceso correcto.
  - La información llegue a su destino y con la persona correcta.
  - Implementen sistemas alternativos de transmisión entre diferentes puntos (Sandoval Quino, 2017).

Mecanismo de seguridad

4. Mecanismo de prevención: Son los que duplican la seguridad cuando se están realizo una tarea para prevenir el robo de información. Ejemplo: El uso de cifrado en la trasmisión de datos porque evita que un atacante escuche las conexiones de un sistema de red (Gutiérrez et al., 2018).
5. Mecanismo de detección: Permite detectar a tiempo las vulnerabilidades de seguridad que se puedan presentar: Ejemplo: El programa de auditoría de Tripwire (Cadavid Romero, 2018).
6. Mecanismo de recuperación: Son aquellos que se utilizan cuando sufren violación en el sistema donde se logra detectar que está surgiendo un problema. Ejemplo: Cuando se implementan las copias de seguridad o el uso de hardware adicional (Patiño et al., 2017).

Los mecanismos de seguridad más implementada en un sistema distribuido:

Cifrado de mensajes

Modo simétrico es cuando su clave se encuentra de modo secreta (Ver Figura 2).

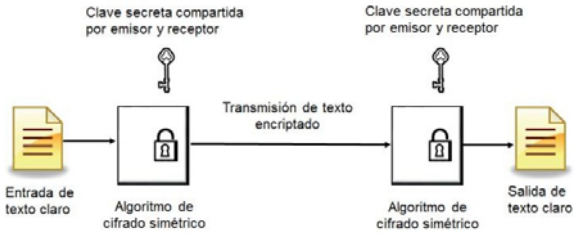

Figura 2. Encriptado Simétrico.

Fuente: (Ramírez & de Asís López-Fuentes, 2017).

Modo asimétrico es cuando su clave se encuentra de modo público y privado (Ver figura 3).

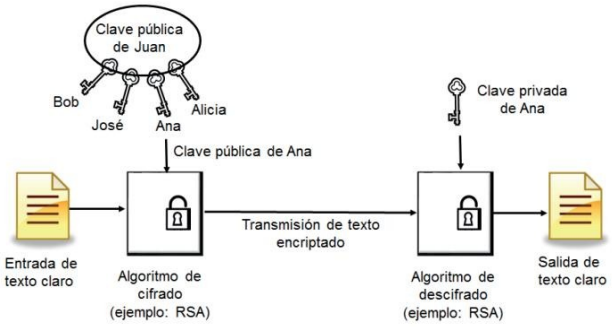

Figura 3. Encriptado asimétrico.

Fuente: (Ramírez & de Asís López-Fuentes, 2017).

1. **Autenticación:**

- Sistemas centralizados: Deben realizar contraseñas por sesiones y están bajo el control del mismo Kernel.
- Sistemas distribuidos: Cumplen con el funcionamiento de Criptografía que se basa en descifrar claves secretas (Santos Carrazana, 2019).

2. **Control de acceso:**
   - Implementa el uso de firewalls y mecanismo para restringir los accesos a personas que no estén autorizadas al ingreso del sistema o información (Alonso et al., 2017).
3. **Firmas digitales:**
   - Evita que un mensaje sea modificado y garantizar él envió de la información (Gallardo et al., 2019).

Resultados y discusión

Los recursos disponibles en la red se utilizan al mismo tiempo por los usuarios que interactúan en la misma.

- En hardware: impresoras y discos.
- En software: ficheros, base de datos.
- Carencia de reloj global: Se necesita temporización para coordinar o sincronizar la transferencia de mensajes.
- Transparencia: Se refiere a la ocultación tanto al usuario y al programador de aplicaciones de la separación de los dispositivos de un sistema distribuido, de manera que el sistema se vea como un todo, en vez de un conjunto de componentes independientes.
- Fallos independientes de los componentes: Cada dispositivo del sistema puede fallar de modo independiente, mientras que los restantes continúan ejecutando sus deberes, por lo tanto, permite que las tareas muestren su mayor efectividad, pues el sistema en su conjunto continúa trabajando (Grillo et al., 2017).

Ventajas:

- El costo y el rendimiento son reducidos porque cada dispositivo del sistema se desenvuelve individualmente.
- Modularidad: cada entidad es independiente y programada para que tenga un óptimo desempeño.
- Capacidad de crecimiento (Escalabilidad).

- Expandible, es decir, se puede agregar nuevos dispositivos como procesadores y servidores que incrementa la capacidad de almacenamiento del sistema.
- Uso de nuevas interfaces.
- Eficiencia y flexibilidad.
- Los recursos actuales no afectan.
- Confiabilidad: El sistema es consistente, aun si una computadora del sistema deja de funcionar.
- Velocidad: Un sistema distribuido puede tener mayor poder de cómputo que una computadora centralizada individual (Pérez Tijero & Gutiérrez, 2017).

Desventajas:

- Requerimientos de mayores controles de procesamiento.
- Velocidad de propagación de información, es decir muy lentas en algunas ocasiones.
- La red de interconexión tiene problema como la latencia
- Seguridad se requiere mejores esquemas de protección para mejorar el acceso a información confidencial o secreta.
- La falta de estándares puede ocasionar inconvenientes de compatibilidad e interconectividad, esto es debido a que se crean muchas copias de la misma aplicación.
- Administración más compleja.
- Servicios de replicación de datos y servicios con posibilidades de fallas (Pessolani et al., 2020).

Ejemplo práctico

Máquina virtual Ubuntu: Cifrar fichero mediante el algoritmo Asimétrico con el comando de Linux GPG. La figura 4 muestra una representación del proceso de ejecución del ejemplo práctico.

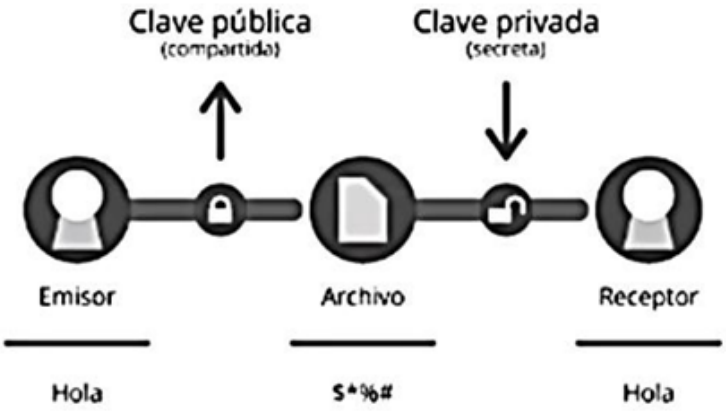

Figura 4. Proceso de ejecución del ejemplo práctico.

La figura 5 muestra una representación de la máquina virtual con dos usuarios, Emisor (Marcos) y Receptor (Nicole).

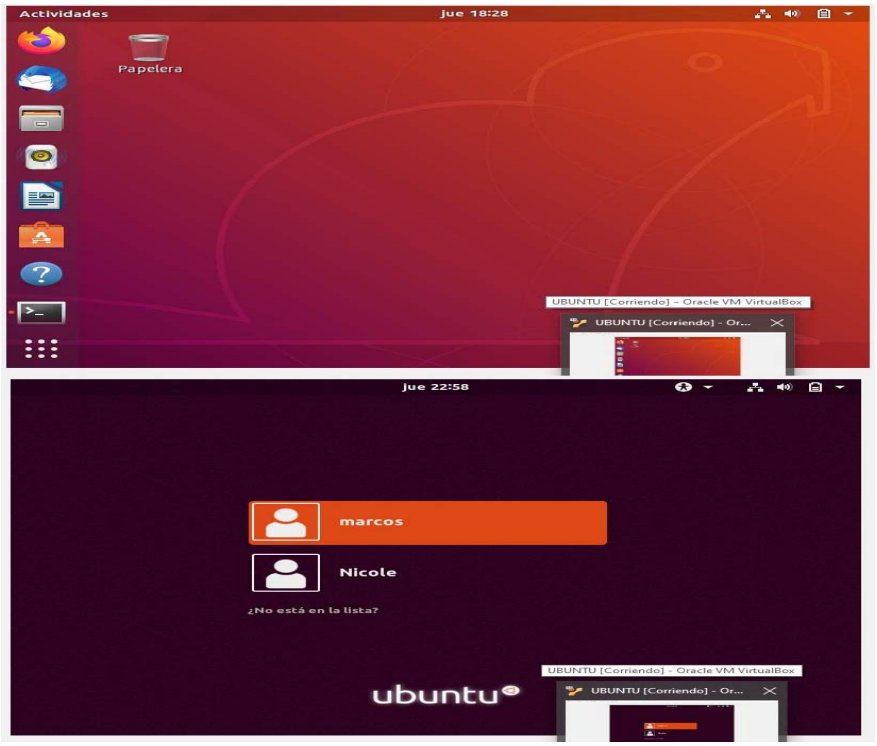

Figura 5. Representación de la máquina virtual con dos usuarios, Emisor (Marcos) y Receptor (Nicole).

La figura 6 muestra una imagen en la forma de generar las claves Pública y Privada, creando un usuario y contraseña.

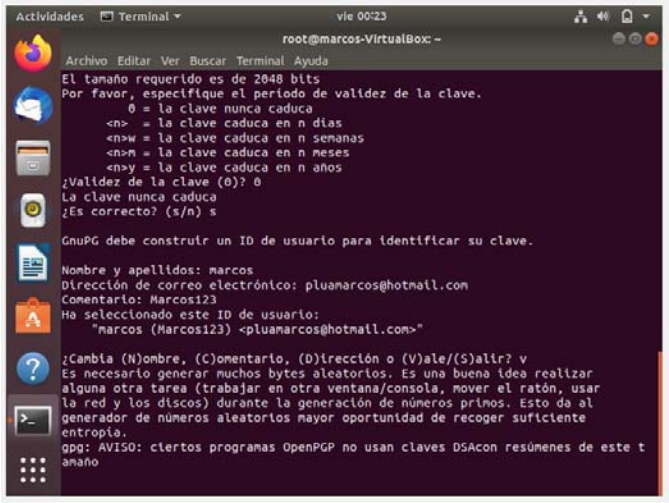

Figura 6. Generar las claves Pública y Privada, creando un usuario y contraseña.

La figura 7 muestra el comando, con el cual se logra observar el Usuario creado, la clave privada y pública.

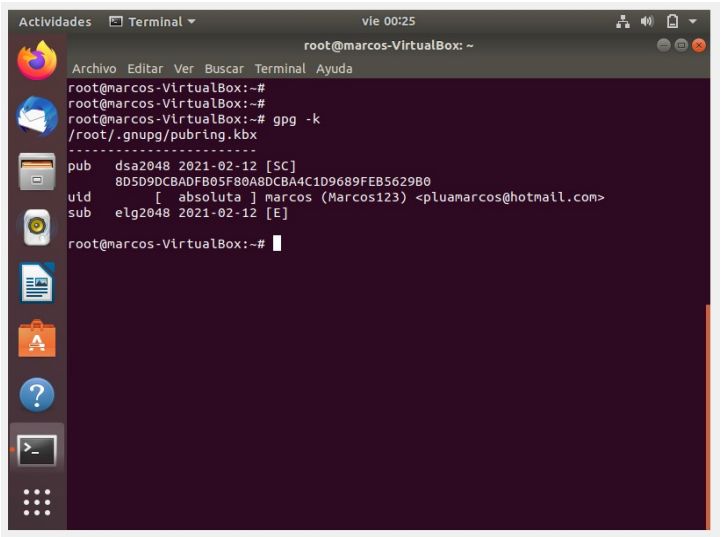

Figura 7. Se logra observar el Usuario creado, la clave privada y pública.

La figura 8 muestra el proceder para exportar la clave pública para poder enviarla a otros usuarios, en este caso al usuario (Nicole).

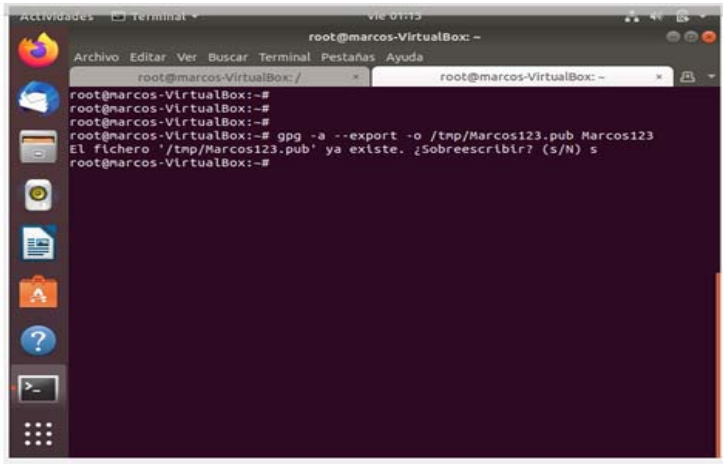

Figura 8. Imagen de exportar la clave pública para poder enviarla a otros usuarios.

Se procede ir al Usuario (Nicole) para importar la clave. La figura 9 visualiza las claves importadas.

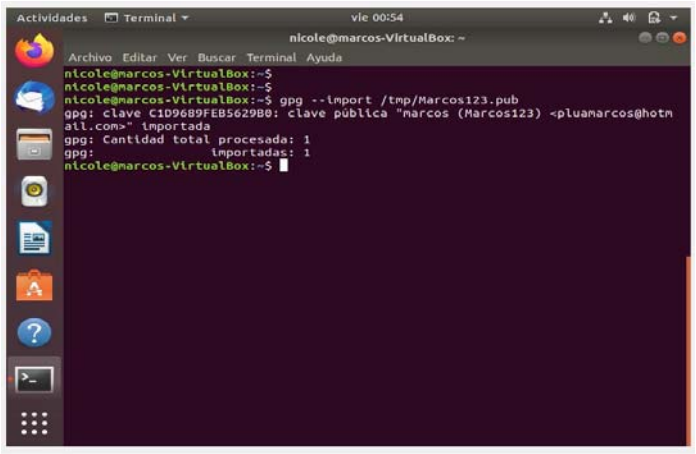

Figura 9. Visualizar claves importadas.

Con el siguiente comando se logra visualizar todos los usuarios creados.

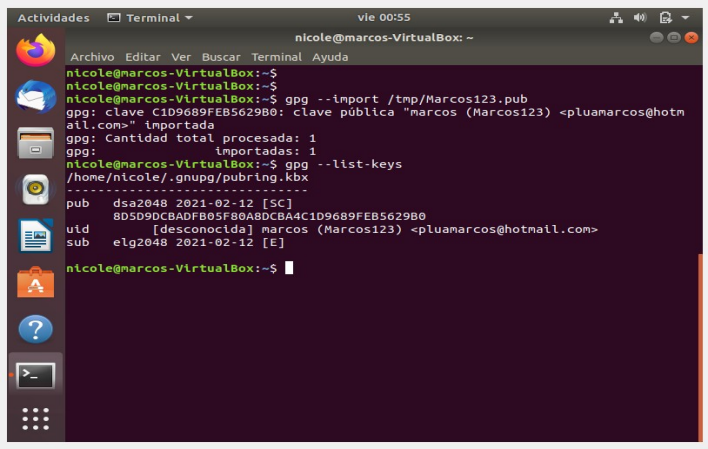

Figura 10. Visualizar todos los usuarios creados.

En este punto es posible generar un mensaje desde el usuario secundario al usuario inicial. Se utiliza un mensaje cifrado con el texto: “MÉTODO ASIMÉTRICO CON ÉXITO”.

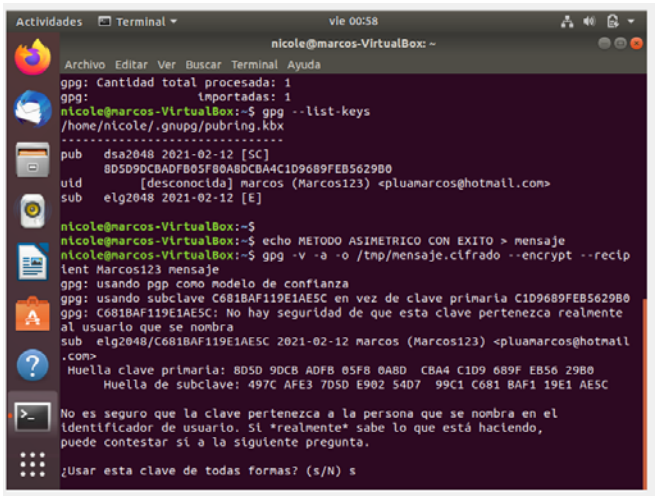

Figura 11. Generar un mensaje desde el usuario secundario al usuario inicial

Se crea un archivo (mensaje cifrado), donde se logra visualizar que el mensaje está cifrado. La figura 12 muestra el archivo creado.

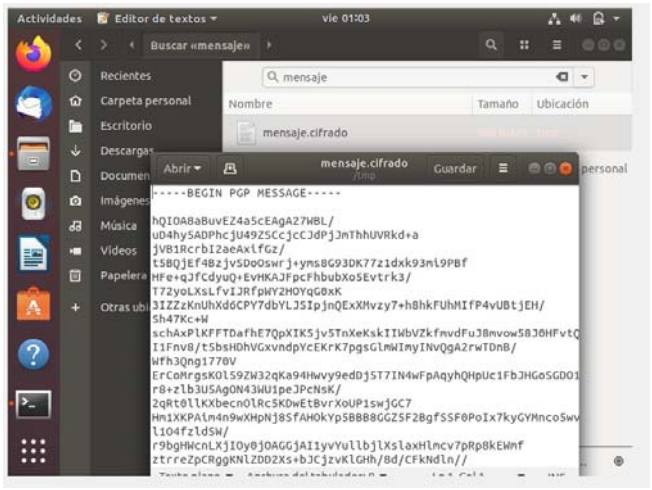

Figura 13. Mensaje cifrado.

En este punto, el Usuario inicial logra observar el mensaje desencriptando. La figura 14 muestra el mensaje desencriptando.

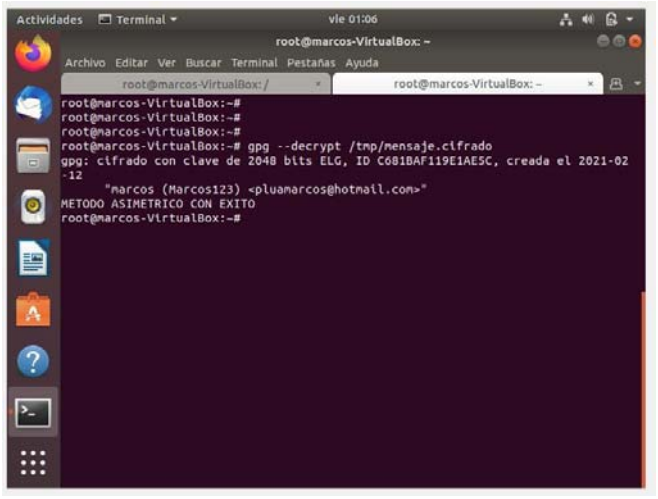

Figura 14. Mensaje des encriptado.

Conclusiones

Los ataques a la seguridad son partes de la realidad de los sistemas distribuidos, por lo cual los usuarios deben tomar las debidas precauciones para que la información esté protegida. Los sistemas distribuidos trabajan de modo transparente y observan el funcionamiento de los usuarios.

Para brindar una mayor seguridad se debe analizar los tres pilares de seguridad como su confidencialidad, disponibilidad y la integridad. La seguridad en sistema distribuido es tener presente los tres componentes como son los datos, la parte de hardware y software. Analizar los mecanismos de seguridad de manera detallada para que la base de datos se encuentre segura.

Recomendaciones

La seguridad en sistema distribuido consiste en mejorar las técnicas de manejo como es efectuar un análisis de riego, mantener los equipos actualizados como sus programas y sus licencias, implementar la seguridad en todos los niveles de como guardar un respaldo de información o establecer planes de contingencia.

La seguridad obliga establecer una correcta contraseña para que solo las personas autorizadas puedan tener acceso a dicha información y crear un establecimiento de políticas.

Conflictos de intereses

Los autores de la presente investigación declaran que no poseen conflictos de intereses.

Contribución de los autores

Conceptualización: Jenny Arízaga-Gamboa, Eduardo Alvarado-Unamuno, Jorge Chicala- Arroyave.

Curación de datos: Jenny Arízaga-Gamboa, Eduardo Alvarado-Unamuno, Jorge Chicala- Arroyave.

Análisis formal: Jenny Arízaga-Gamboa, Eduardo Alvarado-Unamuno.

Investigación: Jenny Arízaga-Gamboa, Eduardo Alvarado-Unamuno.

Metodología: Eduardo Alvarado-Unamuno, Jorge Chicala- Arroyave.

Administración del proyecto: Jenny Arízaga-Gamboa.

Software: Jorge Chicala- Arroyave.

Supervisión: Jenny Arízaga-Gamboa.

Validación: Eduardo Alvarado-Unamuno.

Visualización: Jorge Chicala- Arroyave.

Redacción – borrador original: Jenny Arízaga-Gamboa, Eduardo Alvarado-Unamuno, Jorge Chicala-Arroyave.

Redacción – revisión y edición: Jenny Arízaga-Gamboa, Eduardo Alvarado-Unamuno, Jorge Chicala-Arroyave.

Financiamiento

La investigación no requirió fuente de financiamiento, ha sido financiada por los autores.

Referencias

Alonso, C. G. M., Rafael, S. F., Francisco, M. P., Gabriel, D. O., Elio, S. R., Miguel, S. P. V., Javier, S. B., María, F. A. J., Pau, M. C., & Gregorio, Y. C. J. (2017). *Comunicaciones industriales: sistemas distribuidos y aplicaciones*. Editorial UNED.

Areitio Bertolín, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Editorial Paraninfo.

Cadavid Romero, D. F. (2018). Hallazgos de vulnerabilidades en los sistemas operativos y base de datos de la empresa ALDIM Acciones Logísticas en Distribución de Mercancías SAS.

Carretero Pérez, J., De Miguel Anasagasti, P., García Carballeira, F., & Pérez Costoya, F. (2001). Sistemas Operativos. Una Visión Aplicada. *Mac Graw Hill*.

Estupiñan, A. d. C. A., Pulido, J. A., & Jaime, J. A. B. (2013). Análisis de Riesgos en Seguridad de la Información. *Ciencia, innovación y tecnología*, *1*, 40-53.

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. *Polo del Conocimiento*, *2*(12), 145-155.

Gallardo, I., Bazan, P., & Venosa, P. (2019). Arquitectura de Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada. *Revista Ibérica de Sistemas e Tecnologias de Informação*(32), 49-66.

Grillo, M., Pereira, W., & Cardinale, Y. (2017). Seguridad para la Autentificación, Cifrado y Firma en la Ejecución de Servicios Web Compuestos.(P. 106-118). *Tekhné*, *1*(18).

Gutiérrez, G. V. R., Jaime, J. A. B., & González, I. A. D. (2018). Gestión de seguridad de la información en las organizaciones. *Investigación e Innovación*, *111*.

López Espinoza, H. T. (2012). *Sistema de información geográfica aplicado al catastro de agua potable del Cantón Paute, Ecuador* Quito, 2012.].

Patiño, S., Mosquera, C., Suárez, F., & Nevarez, R. (2017). Evaluación de seguridad informática basada en ICREA e ISO27001. *Universidad Ciencia y Tecnología*, *21*(85).

Pérez Rueda, G. J. (2017). *Estudio de Seguridad informática en el Sistema Académico del Ministerio de Educación* Babahoyo: UTB].

Pérez Tijero, H., & Gutiérrez, J. J. (2017). DDS en el desarrollo de sistemas distribuidos heterogéneos con soporte para criticidad mixta. *Actas de las XXXVIII Jornadas de Automática*.

Pessolani, P., Harispe, D. G., & Garcia Aguirre, O. (2020). Localización y seguimiento de servicios replicados en un sistema de virtualización distribuido.

Ramírez, J. A. I., & de Asís López-Fuentes, F. (2017). Autenticación para acceso a datos distribuidos basado en Kerberos. *Res. Comput. Sci.*, *142*, 69-78.

Sandoval Quino, J. P. (2017). Diseño de un Plan de Seguridad de la Información para el Centro de Informática y Telecomunicaciones de la Universidad Nacional de Piura, Periodo 2015-2018.

Santos Carrazana, A. (2019). *Los sistemas distribuidos. Una aplicación en la enseñanza* Universidad Central "Marta Abreu" de Las Villas].

Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL*, *28*(5).

Vera, V. D. G., & Vera, J. C. G. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia et technica*, *22*(2), 193-197.

Villacís, G. V., & Morocho, R. A. R. (2017). Vulnerabilidades y amenazas a los servicios web de la intranet de la universidad técnica de Babahoyo. *3c Tecnología: glosas de innovación aplicadas a la pyme*, *6*(1), 53-66.