IMPLEMENTACIÓN DE REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO EN ENDIAN FIREWALL

Yorladys Palacio Cordoba
e-mail: ypalaciocor@unadvirtual.edu.co

RESUMEN: *Este artículo presenta el desarrollo de un laboratorio práctico orientado a la implementación de reglas de acceso mediante GNU/Linux Endian Firewall Community para controlar y supervisar el tráfico entre diferentes segmentos de red. La práctica se ejecutó en un entorno virtualizado con Oracle VirtualBox, utilizando una arquitectura compuesta por las zonas GREEN (LAN), ORANGE (DMZ) y RED (WAN). El objetivo principal fue configurar políticas de seguridad que permitieran autorizar y denegar comunicaciones mediante los protocolos HTTP y FTP, utilizando los puertos 80 y 21. Asimismo, se realizaron pruebas de conectividad, monitoreo de tráfico Inter-Zona y validación de las reglas configuradas desde clientes, servidores y redes externas. Los resultados obtenidos demostraron el correcto funcionamiento de las políticas implementadas y evidenciaron que la segmentación de red y el uso de mecanismos de filtrado fortalecen la seguridad, optimizando el control de las comunicaciones y reduciendo riesgos de acceso no autorizado en entornos empresariales.*

PALABRAS CLAVE: Endian, Firewall, Reglas de acceso, Tráfico

1 INTRODUCCIÓN

Los sistemas de firewall representan herramientas fundamentales para garantizar la seguridad en las infraestructuras de red, debido a que permiten supervisar y controlar el flujo de información entre diferentes segmentos mediante políticas de filtrado y control de acceso. Estas políticas posibilitan autorizar o restringir conexiones según parámetros previamente definidos, fortaleciendo la protección frente a accesos no autorizados y vulnerabilidades.

Asimismo, la segmentación en zonas LAN, WAN y DMZ contribuye a mejorar la administración de servicios y fortalecer la seguridad perimetral, al separar los recursos internos de los servicios expuestos a redes externas. Durante esta práctica se realizó la instalación y configuración de Endian Firewall Community en VirtualBox, con el objetivo de implementar políticas de comunicación mediante los protocolos HTTP y FTP. Además, se efectuaron pruebas de conectividad y monitoreo del tráfico Inter-Zona para verificar el correcto funcionamiento de las reglas configuradas entre clientes, servidores y redes externas.

2 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

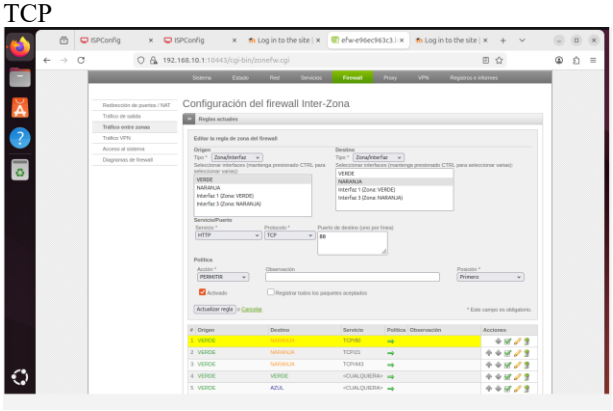
Las reglas de acceso en un Firewall representan un mecanismo fundamental dentro de la seguridad perimetral, debido a que permiten controlar y supervisar el tráfico de datos entre diferentes segmentos de red mediante políticas de filtrado previamente definidas [1], [2]. Estas políticas permiten autorizar o denegar conexiones según parámetros como dirección IP, protocolo, puerto y tipo de servicio, fortaleciendo la protección de la infraestructura tecnológica y reduciendo riesgos asociados a accesos no autorizados [3], [4].

2.1 COMUNICAR LA ZONA VERDE CON LA ZONA NARANJA, MEDIANTE LOS PROTOCOLOS HTTP Y FTP, CON SUS RESPECTIVOS PUERTOS.

La configuración de reglas de acceso entre la zona GREEN (LAN) y la zona ORANGE (DMZ) permitió habilitar la comunicación mediante los protocolos HTTP y FTP utilizando los puertos 80 y 21, respectivamente [5]. Para ello, se ingresó a la interfaz administrativa de Endian Firewall Community y se definieron políticas especificando origen, destino, protocolo y acción de permitir tráfico.

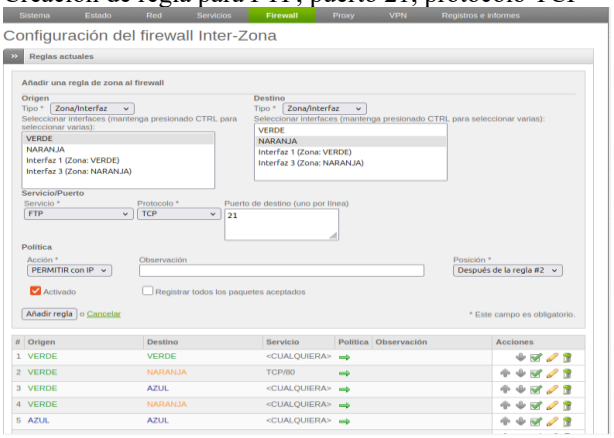
Posteriormente, se realizaron pruebas de conectividad desde el cliente ubicado en la red interna hacia el servidor alojado en la DMZ, verificando el acceso correcto a los servicios web y FTP. Según Lemus et al. [6], la implementación de reglas específicas entre zonas segmentadas fortalece la seguridad perimetral y facilita el control de acceso a los servicios empresariales. Además, se comprobó que únicamente los puertos autorizados podían establecer comunicación entre las zonas configuradas. Las Figuras 1 y 2 presentan las reglas configuradas, mientras la Figura 3 muestra la conexión entre el cliente LAN y el servidor DMZ.

Figura 1.
Creación de regla para de HTTP, puerto 80, protocolo TCP



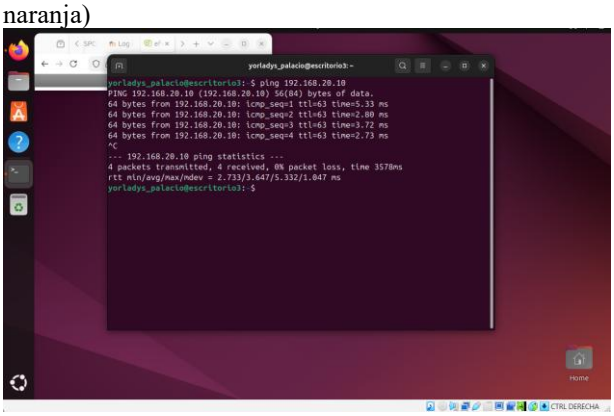
Fuente: Autoría Propia

Figura 2
Creación de regla para FTP, puerto 21, protocolo TCP



Fuente: Autoría Propia

Figura 3.
Conexión del cliente (zona verde) con el DMZ (zona naranja)



Fuente: Autoría Propia

2.2 COMUNICAR LA ZONA INTERNET CON LA ZONA DMZ.

La comunicación entre la zona Internet (RED/WAN) y la DMZ se configuró mediante reglas de Firewall orientadas a permitir únicamente el acceso autorizado al servidor publicado en la zona desmilitarizada [7]. Para ello, se definieron políticas específicas asociadas a la dirección IP 192.168.20.10 del servidor DMZ y al protocolo HTTP utilizando el puerto 80. Esta configuración evitó la exposición innecesaria de servicios y contribuyó al fortalecimiento de la seguridad perimetral.

Según Fulp [8], los firewalls permiten controlar el tráfico entre redes externas e internas mediante políticas de filtrado y segmentación, donde la DMZ funciona como una zona intermedia destinada a publicar servicios accesibles desde Internet sin exponer directamente la red local. Posteriormente, se realizaron pruebas de acceso desde redes externas hacia el servidor web alojado en la DMZ para validar la funcionalidad de las reglas configuradas. Asimismo, se verificó el correcto direccionamiento del tráfico proveniente de Internet hacia el servidor autorizado. La Figura 4 presenta la regla configurada para permitir el acceso HTTP desde la zona WAN hacia la zona DMZ.

Figura 4.
Creación de la regla de acceso para permitir el tráfico proveniente de la zona Internet hacia la zona DMZ.

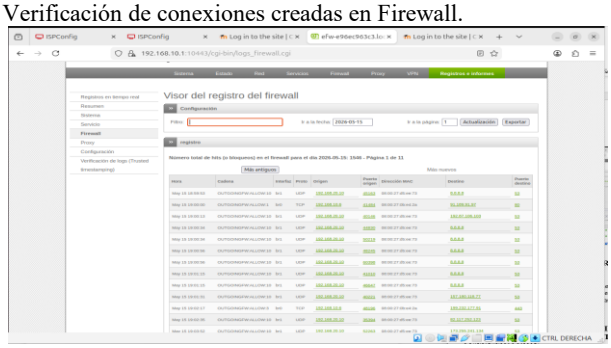
Fuente: Autoría Propia

2.3 VERIFICAR EN EL TRÁFICO INTER - ZONA, LA CREACIÓN DE LAS REGLAS.

La verificación del tráfico Inter-Zona permitió comprobar el correcto funcionamiento de las políticas de acceso implementadas en el Firewall [9]. Para ello, se utilizaron las herramientas de monitoreo y registro integradas en Endian Firewall Community, observando el comportamiento del tráfico entre las zonas GREEN, ORANGE y RED.

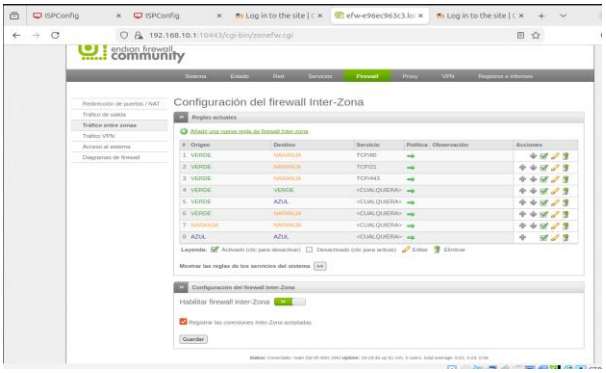
Según Marín et al. [4], la supervisión continua de las reglas de Firewall fortalece la seguridad informática y facilita la detección de accesos no autorizados. Durante la práctica se verificó que únicamente las conexiones asociadas a protocolos y puertos permitidos eran aceptadas. Además, se analizaron los registros generados por el Firewall para validar la trazabilidad de las conexiones entre clientes, servidores y redes externas. La Figura 5 muestra la verificación de conexiones creadas en el Firewall, mientras que la Figura 6 presenta el monitoreo del tráfico Inter-Zona.

Figura 5.
Verificación de conexiones creadas en Firewall.



Fuente: Autoría Propia

Figura 6.
Verificación de conexiones de la configuración del Firewall Inter-Zona.



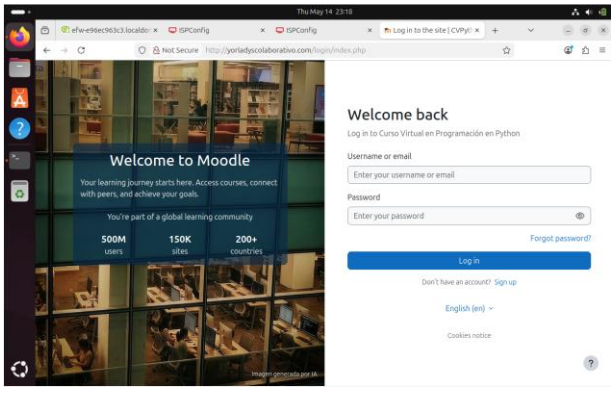
Fuente: Autoría Propia

2.4 PROBAR DESDE UN NAVEGADOR WEB LAS SIGUIENTES DIRECTIVAS:

Con el fin de validar las políticas de acceso configuradas en el Firewall, se realizaron diferentes pruebas de conectividad desde los distintos segmentos de red utilizando navegadores web y servicios FTP y HTTP [2]. Estas verificaciones permiten comprobar el correcto funcionamiento de las reglas establecidas entre las zonas LAN, WAN y DMZ, garantizando la comunicación autorizada entre las diferentes interfaces de red.

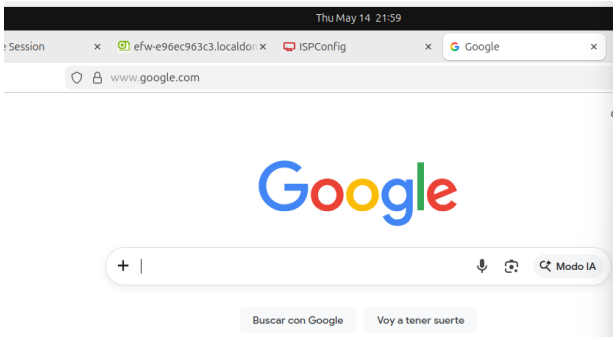
Según LaCroix [11], las pruebas de conectividad representan una etapa fundamental en la administración de servidores y redes GNU/Linux, debido a que facilitan la detección de errores de configuración y permiten garantizar la disponibilidad de los servicios implementados. En la Figura 7 se evidencia el acceso HTTP desde la zona LAN hacia la DMZ, ingresando la url de la IP del servidor, http://192.168.20.10 o el dominio del sitio web http://yorladyscolaborativo.com en el navegador, mientras que la Figura 8 muestra la comunicación HTTP desde la LAN hacia la WAN, accediendo al sitio web de Google.

Figura 7.
Acceso HTTP de la zona LAN hacia la zona DMZ.



Fuente: Autoría Propia

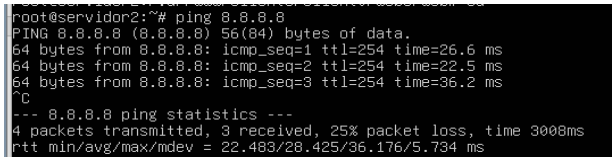
Figura 8.
Acceso HTTP desde la zona LAN hacia la zona WAN.



Fuente: Autoría Propia

Posteriormente, la Figura 9 presenta la validación del acceso desde la DMZ hacia Internet mediante la utilización del comando ping 8.8.8.8, indicando la dirección IP principal del DNS público de Google en la terminal del servidor web, comprobando el correcto funcionamiento de las políticas de salida configuradas en el Firewall.

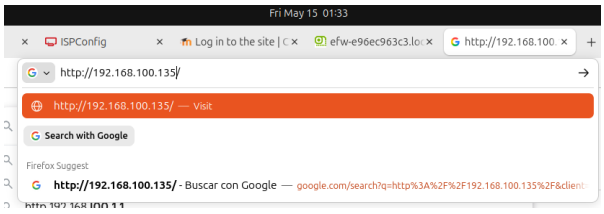
Figura 9
Comprobación del DNS con el comando ping.



Fuente: Autoría Propia

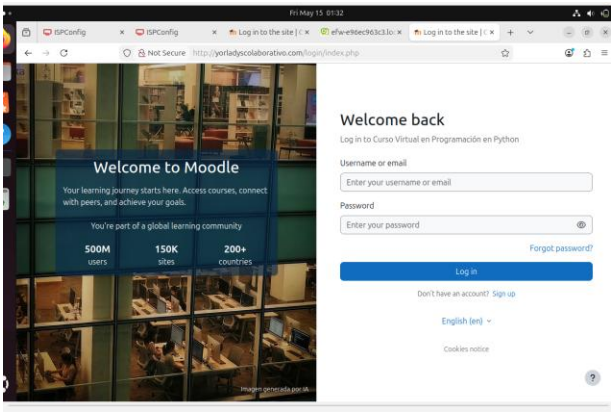
Asimismo, las Figuras 10 y 11 presentan la validación del acceso HTTP desde la WAN hacia la DMZ mediante el ingreso de la dirección IP pública (192.160.100.135) de la zona WAN en el navegador web. Posteriormente, se evidenció la visualización correcta del sitio web alojado en el servidor, comprobando el funcionamiento adecuado de las reglas de acceso configuradas en el Firewall.

Figura 10.
Ingreso de la IP pública de la WAN en el navegador.



Fuente: Autoría Propia

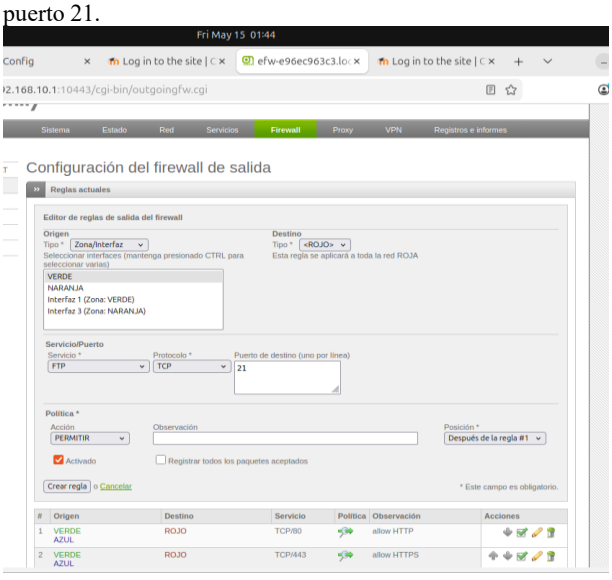
Figura 11.
Visualización del sitio de DMZ. Con la url de http://192.160.100.135



Fuente: Autoría Propia

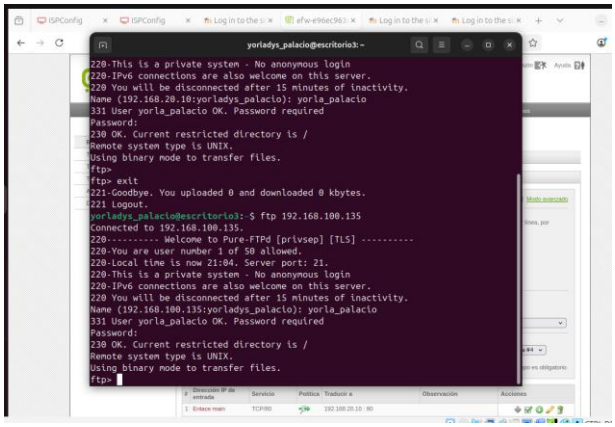
De igual forma, la Figura 12 presenta la regla configurada para permitir la comunicación desde la zona verde hacia la zona roja. Asimismo, la Figura 13 evidencia la validación del servicio FTP desde la LAN hacia la WAN, ingresando con el comando ftp más la dirección IP pública 192.168.100.135 de la zona WAN, en la terminal de Ubuntu Desktop. Posteriormente, el sistema mostró el mensaje de bienvenida y solicitó autentificación mediante usuario y contraseña para ingresar a la gestión de servicio de transporte de archivo. comprobando el correcto funcionamiento de las políticas de acceso establecidas en el Firewall.

Figura 12.
Configuración de regla de salida de zona verde a zona roja, puerto 21.



Fuente: Autoría Propia

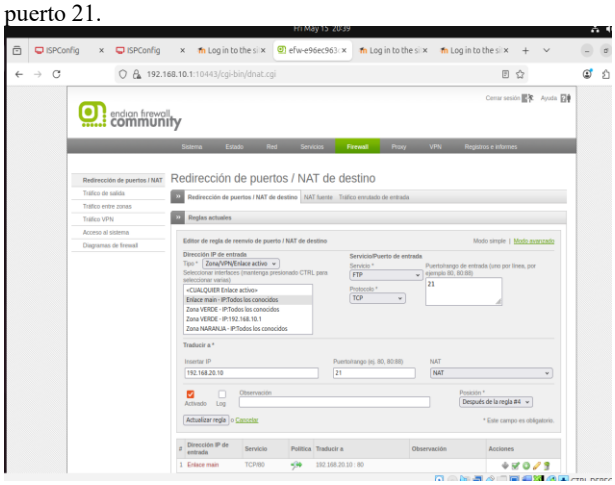
Figura 13.
Acceso FTP en la terminal de la zona verde mediante la IP de WAN.



Fuente: Autoría Propia

La Figura 14 presenta la configuración de la redirección de puertos mediante NAT de destino en la página de Endian, donde se agregó la regla de acceso desde la zona roja hacia la zona naranja, de acuerdo con las políticas de seguridad establecidas.

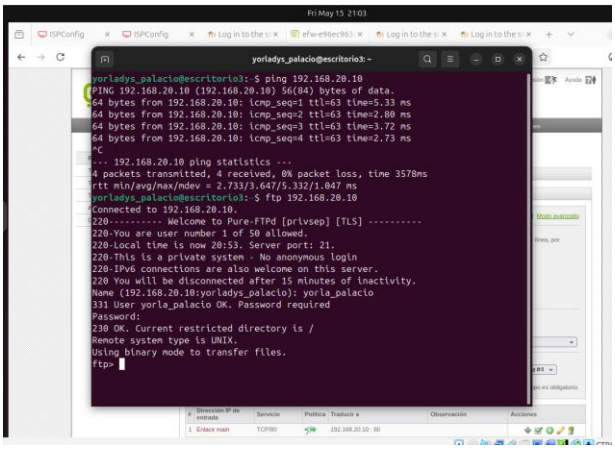
Figura 14.
La configuración de regla de salida de zona roja a la naranja, puerto 21.



Fuente: Autoría Propia

Asimismo, la Figura 15 muestra la validación del servicio FTP desde la WAN hacia la DMZ utilizando el comando FTP y la dirección IP 192.168.20.10 del servidor. Durante la prueba se verificó la conexión a través del puerto 21, permitiendo la autenticación mediante usuario y contraseña, así como la transferencia de archivos. Los resultados obtenidos evidenciaron la efectividad del Firewall para controlar y filtrar el tráfico de red de acuerdo con las políticas de seguridad establecidas.

Figura 15.
Acceso de FTP con la IP del servidor DMZ.



Fuente: Autoría Propia

3 CONCLUSIONES.

La implementación de reglas de acceso en Endian Firewall Community permitió controlar de manera eficiente el tráfico entre las zonas LAN, WAN y DMZ mediante los protocolos HTTP y FTP, fortaleciendo la seguridad perimetral de la infraestructura de red. Las pruebas de conectividad realizadas evidenciaron que las políticas configuradas autorizaron únicamente las conexiones definidas según los parámetros establecidos, garantizando un adecuado control del acceso a los servicios. Asimismo, el monitoreo del tráfico Inter-Zona facilitó la verificación del correcto funcionamiento de Endian Firewall y la validación de las comunicaciones entre clientes, servidores y redes externas. En consecuencia, la práctica permitió consolidar conocimientos relacionados con la administración de políticas de seguridad, segmentación de redes y control de tráfico en entornos GNU/Linux virtualizados.

4 REFERENCIAS

[1] Endian, Endian UTM 3.2 Manual Reference. *Endian*, 2016. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html

[2] Canonical, Help Ubuntu. *Ubuntu*, 2023. [En línea]. Disponible en: https://help.ubuntu.com/

[3] R. K. Sharma, H. K. Kalita y B. Issac, "Different Firewall Techniques: A Survey," en Proc. 5th Int. Conf. Computing Communication and Networking Technologies (ICCCNT), 2014, pp. 1–6. [En línea]. Disponible en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/stamp/stamp.jsp?tp=&arnumber=6963102

[4] J. J. Marín Valencia, A. Patiño Valencia, y J. C. Acevedo Bedoya, "Implementación de un sistema de seguridad perimetral informático usando VPN, Firewall e IDS", *Rev. Univ. Catol. Oriente*, vol. 31, n.º 45, pp. 84–99, sep. 2020. [En línea]. Disponible en: https://doi.org/10.47286/01211463.284

[5] Oracle, Manual de usuario de VirtualBox. *Oracle VM VirtualBox*, 2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/

[6] M. V. Lemus, et al. Implementación de zona desmilitarizada (DMZ) y políticas de acceso en Endian Firewall para intranets gnu/linux, con el fin de optimizar la seguridad perimetral. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/76971.

[7] "Firewall and DMZ Design: Check Point," *en Designing and Building Enterprise DMZs*. Amsterdam, Países Bajos: Elsevier, 2006, pp. 315–353. [En línea]. Disponible en: https://research.ebsco.com/plink/953ec124-f380-3af3-8a41-b058f7d799a1

[8] E. W. Fulp, "Firewalls," in Computer and Information Security Handbook, Elsevier Inc., 2009, pp. 349–367. [En línea]. Disponible en: https://doi.org/10.1016/B978-0-12-374354-1.00021-2

[9] F. H. Cepeda-López, "La topología de redes como herramienta de seguimiento en el sistema de pagos de alto valor en Colombia," *Borradores de Economía*, no. 513, Banco de la República de Colombia, 2008. [En línea]. Disponible en: https://doi.org/10.32468/be.513

[10] J. LaCroix, Mastering Ubuntu Server: *Gain* Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server. Birmingham, Reino Unido: Packt Publishing, 2020. [En línea]. Disponible en: https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952