IMPLEMENTACIÓN Y ADMINISTRACIÓN DE SISTEMAS GNU/LINUX: DESDE LA SEGURIDAD PERIMETRAL HASTA LA GESTIÓN DE SERVICIOS

Luis Felipe Rodriguez Martínez
e-mail : lfrodriguez@unadvirtual.edu.co

RESUMEN: *Este artículo presenta una visión integrada sobre la implementación y administración de sistemas GNU/Linux en entornos virtualizados, destacando su uso como plataforma robusta para la seguridad perimetral, la segmentación de red y la gestión de servicios críticos. Se emplea Endian Firewall Community (EFW) como herramienta central para configurar redes seguras con zonas GREEN (LAN), ORANGE (DMZ) y RED (WAN), gestionando tráfico, autenticación y servicios web. Además, se abordan prácticas esenciales de administración de GNU/Linux: gestión de usuarios, servicios de red, respaldos, virtualización, y automatización de tareas, alineadas con estándares de seguridad como ISO/IEC 27001.*

PALABRAS CLAVE:GNU/Linux,Endian Firewall, VirtualBox, Respaldo.

1 INTRODUCCIÓN

La creciente demanda de redes seguras y escalables ha posicionado a GNU/Linux como un sistema operativo líder en infraestructuras empresariales. Endian Firewall Community, basado en GNU/Linux, ofrece una solución de seguridad perimetral que unifica múltiples funciones en una plataforma UTM (Unified Threat Management). Este trabajo desarrolla un entorno virtualizado con VirtualBox, donde se implementa EFW para segmentar redes y permitir el acceso controlado a servicios HTTP/FTP desde la DMZ, bloquear protocolos no deseados como ICMP, y aplicar reglas de acceso entre zonas. Complementariamente, se abordan conceptos fundamentales de administración en GNU/Linux, fortaleciendo las competencias en el manejo de sistemas abiertos.

1.1 SEGURIDAD PERIMETRAL CON ENDIAN FIREWALL COMMUNITY EFW

se erige como una plataforma UTM basada en GNU/Linux, diseñada para unificar funciones críticas de seguridad en un sistema integrado. Más allá de su capacidad de firewall, EFW incorpora proxy HTTP/HTTPS, prevención de intrusiones (IDS/IPS), filtrado de contenido web y servidores VPN [4].

1.2 OBJETIVOS CLAVES

Establecer una arquitectura segmentada (RED, ORANGE, GREEN) que permita separar físicamente los distintos niveles de exposición y funcionalidad de los servicios, facilitando el control del tráfico, la inspección de paquetes y la aplicación de políticas específicas por zona.

Aplicar QoS y filtrado de contenido para optimizar el rendimiento de la red, garantizando una priorización adecuada del tráfico crítico, reduciendo el ancho de banda mal utilizado y fortaleciendo el entorno frente a accesos no deseados.

Unificar autenticación mediante LDAP/AD, permitiendo la centralización del control de identidades y accesos, mejorando la trazabilidad y facilitando la gestión de usuarios en entornos empresariales complejos.

Implementar VPN seguras (OpenVPN, IPsec) con el fin de establecer canales cifrados que aseguren la integridad y confidencialidad de la información transmitida entre sedes remotas o usuarios móviles, apoyando esquemas de trabajo híbrido y acceso remoto seguro.

Integrar monitoreo de tráfico en tiempo real para anticipar comportamientos anómalos o intentos de intrusión, fortaleciendo la vigilancia proactiva del entorno perimetral.

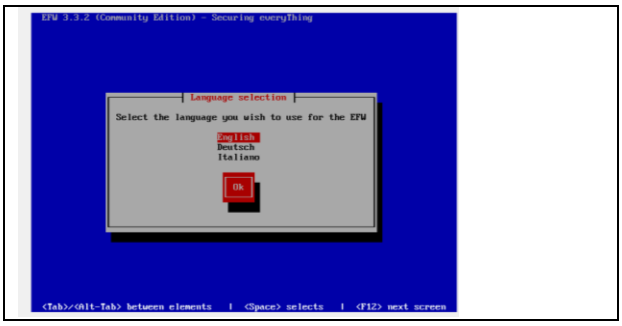
2 INSTALACIÓN Y CONFIGURACIÓN PREPARACIÓN DEL ENTORNO VIRTUAL

Se utilizó VirtualBox como hipervisor, creando una máquina virtual para EFW con los siguientes requisitos: 1 núcleo CPU, 2048 MB de RAM, 20 GB de disco, y tres adaptadores de red:
Adaptador 1 (GREEN): red interna “CLIENTE”.
Adaptador 2 (ORANGE): red interna “SERVIDOR”.
Adaptador 3 (RED): NAT para acceso a Internet.

2.1 ASIGNACIÓN DE ZONAS Y CONFIGURACIÓN INICIAL

Tras montar la ISO de EFW, se sigue el instalador en modo texto. característica de muchas distribuciones GNU/Linux orientadas a entornos de red. Esta instalación paso a paso.
permite configurar elementos esenciales como el idioma, el tipo de teclado, y la interfaz de red principal. Es fundamental seguir cuidadosamente cada pantalla para garantizar que las zonas GREEN, ORANGE y RED se establezcan correctamente desde el principio. A continuación, se muestra el proceso (Figura 1)

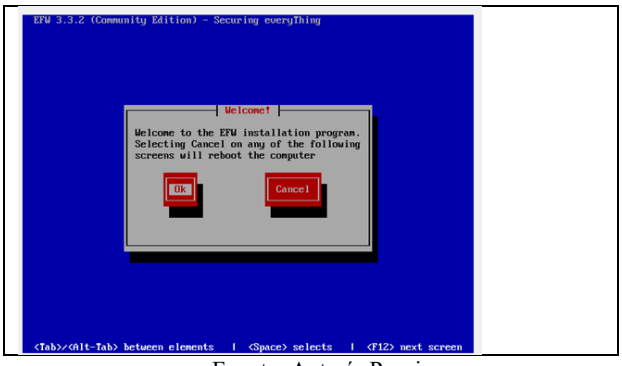
Figura 1. Selección de idioma en EFW



Fuente: Autoría Propia

El primer paso *"ver Figura 2"* formal en el proceso de instalación de Endian Firewall. Desde aquí se inicia el asistente interactivo que guiará al usuario por las configuraciones iniciales. Al presionar 'Ok', el sistema procede con los pasos subsiguientes, mientras que seleccionar 'Cancel' reiniciará automáticamente la máquina virtual.

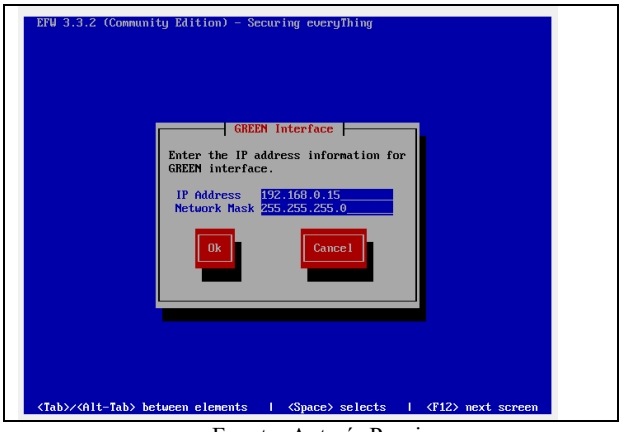
Figura 2. Pantalla de bienvenida al instalador.



Fuente: Autoría Propia

Se solicita al administrador definir manualmente la dirección IP estática y la máscara de subred para la interfaz GREEN (zona LAN). En este ejemplo *"ver Figura 3"*, se asigna la dirección 192.168.0.15 con una máscara de 255.255.255.0. Esta configuración inicial es crucial para asegurar la conectividad posterior entre el firewall y los dispositivos de la red interna.

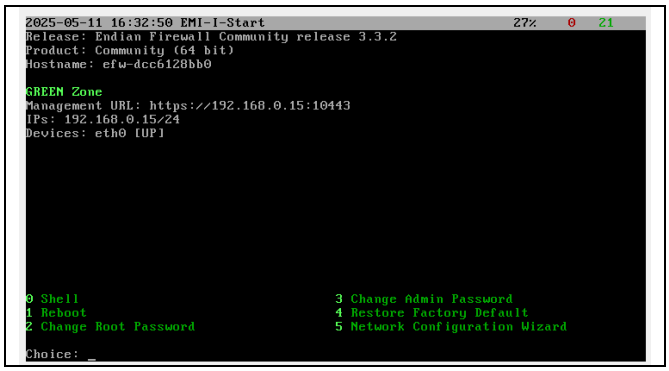
Figura 3. Configuración manual de IP en la interfaz GREEN



Fuente: Autoría Propia

Tras la instalación con detalles de red.
Esta pantalla *"ver Figura 4"* confirma que la instalación de Endian Firewall se ha completado con éxito. Desde aquí, el administrador puede consultar la dirección IP asignada a la zona GREEN, acceder a la interfaz web mediante la URL indicada (https://192.168.0.15:10443), y ejecutar tareas básicas de configuración como el cambio de contraseñas o reinicio del sistema.

Figura 4. Pantalla de bienvenida al instalador.



Fuente: Autoría Propia

La interfaz también muestra el estado de la red y el dispositivo activo (eth0), lo cual es crucial para verificar la conectividad inicial antes de continuar con configuraciones avanzadas.

Luego se accede vía navegador a https:// 192.168.0.15:10443 para completar la configuración.

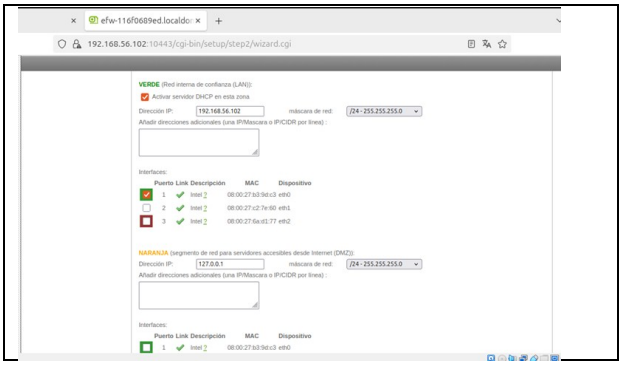
2.2 SEGMENTACIÓN Y CONECTIVIDAD

Se verifica conectividad entre zonas con ping desde un cliente Ubuntu en la zona GREEN, confirmando acceso al firewall. También se implementa un servidor en la zona ORANGE, configurando su red vía netplan**.**

3. CONFIGURACIÓN DE REGLAS NAT Y PORT FORWARDING

Para asegurar la correcta comunicación entre las distintas zonas de red (GREEN, ORANGE y RED), Endian Firewall permite crear reglas de traducción de direcciones (NAT) y redirección de puertos (Port Forwarding). Estas reglas son fundamentales para garantizar el flujo de datos autorizado y seguro entre clientes internos, servidores de la DMZ y el acceso externo a Internet. A través del módulo de firewall de la interfaz web de EFW, es posible definir el origen, destino, protocolo y puerto para cada caso de uso *"ver Figura 5"*.

Figura 5. Panel de configuración de reglas inter-zona



Fuente: Autoría Propia

En el módulo de firewall de EFW.
Desde la interfaz de EFW se crean reglas NAT para permitir tráfico:

GREEN → RED: salida a Internet.

ORANGE → RED: navegación y actualización del servidor.

RED → ORANGE: acceso externo a servicios en la DMZ mediante Port Forwarding.

Ejemplo: Redirección del puerto 80 externo al 192.168.3.10:80 (Apache).

4 HABILITACIÓN DE SERVICIOS EN LA DMZ

4.1 SERVICIO HTTP Y FTP DESDE UBUNTU SERVER EN LA ZONA ORANGE

Se habilitan ambos servicios y se crean reglas en el firewall para permitir el acceso desde la zona GREEN. Para demostrar la correcta implementación de estos servicios, se utilizó phpMyAdmin como herramienta de administración gráfica de bases de datos. Desde esta interfaz se verificó el funcionamiento del servicio web Apache accediendo a través de la red interna, confirmando que la redirección de puertos y las reglas NAT configuradas en Endian permitían la conectividad y operación fluida del servidor web.
En cuanto a la gestión de permisos, los sistemas GNU/Linux emplean el esquema rwx (lectura, escritura y ejecución) para definir los niveles de acceso a archivos y directorios, tanto para el usuario propietario, el grupo asociado y otros usuarios. Herramientas como chmod y chown permiten modificar estos permisos y asignaciones.

4.2 BLOQUEO DE ICMP

Con el objetivo de fortalecer la seguridad perimetral y minimizar la superficie de exposición ante posibles amenazas, se procedió a bloquear el tráfico ICMP (echo-request/reply) entre las distintas zonas definidas en la topología de red. Este protocolo, aunque útil para diagnóstico y pruebas de conectividad, también es comúnmente empleado por atacantes para mapear redes internas y detectar dispositivos activos mediante escaneos automatizados.

A través de la interfaz de administración de Endian Firewall, se crearon reglas específicas dentro del módulo de tráfico inter-zona para denegar explícitamente las solicitudes ICMP entrantes y salientes entre las zonas GREEN, ORANGE y RED. Esta configuración impide el uso del comando ping desde una zona hacia otra, limitando así la capacidad de descubrimiento de hosts y reduciendo la visibilidad de la infraestructura ante exploraciones externas no autorizadas.

Esta política de denegación contribuye a establecer un entorno de red más hermético y resiliente, en concordancia con buenas prácticas recomendadas por marcos normativos como ISO/IEC 27001.

5 IMPLEMENTACIÓN DE PROXY HTTP CON AUTENTICACIÓN

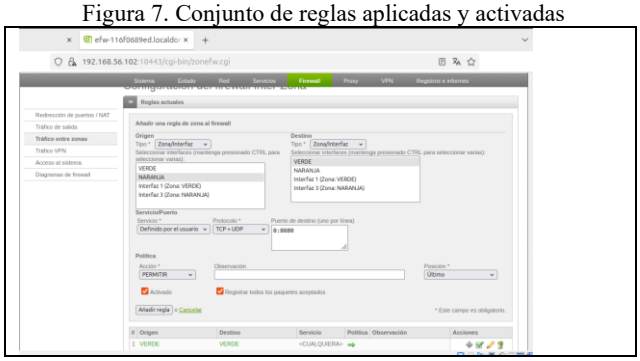
5.1 REGLAS DE ACCESO ENTRE ZONAS

El software libre se basa en cuatro libertades esenciales: ejecutar el programa para cualquier propósito, estudiar cómo funciona y modificarlo, redistribuir copias, y distribuir versiones modificadas. Estas libertades están respaldadas por licencias como la GPL (General Public License) y la licencia.
A continuación*"ver Figura 6 al 7"*, se detalla el conjunto de reglas.

Figura 6. Regla de firewall permitiendo HTTP de LAN a DMZ

Fuente: Autoría Propia

Figura 7. Conjunto de reglas aplicadas y activadas



Fuente: Autoría Propia

Adicionalmente, se creó una regla de tráfico desde la zona ROJA (Internet) hacia la zona NARANJA (DMZ), con el fin

de permitir el acceso público a servicios como servidores web. Este proceso implicó la especificación de protocolo, puerto y zona, así como la priorización de la política de seguridad.
Posteriormente, se realizó una validación en el módulo "Tráfico entre zonas", donde se verificó que las reglas (Figura 8) configuradas habilitaban correctamente el tráfico de interés entre las zonas GREEN, ORANGE y RED.

Figura 8. Prueba de HTTP desde LAN hacia DMZ

Fuente: Autoría Propia

La verificación y validación de estas reglas es clave para garantizar la correcta aplicación de la política de seguridad y mantener la coherencia entre segmentación lógica y funcionalidad operativa. Estas pruebas validan no solo la funcionalidad de red sino también el cumplimiento de los objetivos de segmentación segura y acceso controlado.

5.2 CONFIGURACIÓN DE PROXY HTTP NO TRANSPARENTE

El proxy HTTP no transparente desde la interfaz web de EFW.
Se configura un proxy HTTP no transparente en EFW con autenticación por usuario. Se crean listas negras para restringir sitios como YouTube o redes sociales. Esto refuerza la política de uso aceptable de Internet y mejora el control del ancho de banda.

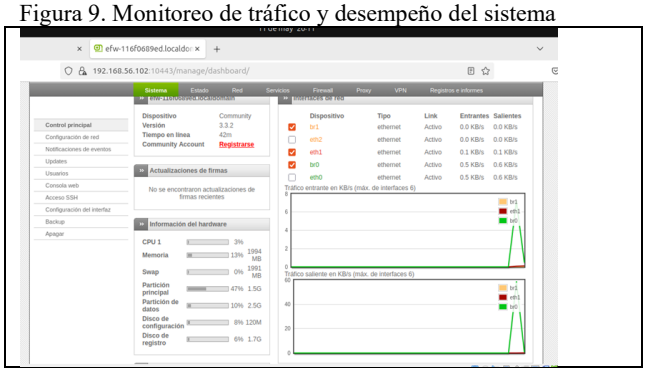
5.3 MONITOREO DE TRÁFICO Y DESEMPEÑO DEL SISTEMA

La interfaz gráfica de Endian Firewall provee herramientas integradas para supervisar en tiempo real el estado del hardware y el tráfico de red. El panel del sistema, donde se despliega información detallada como el uso de CPU, memoria RAM, particiones del disco, estado de las interfaces de red y velocidad de tráfico entrante/saliente por cada interfaz activa (br0, eth1, br1, etc.).

Estos gráficos de actividad permiten detectar patrones de uso anómalos, cuellos de botella, o incluso intentos de ataque que saturen alguna interfaz. Además, se identifican los picos de carga o transferencia, facilitando la toma de decisiones informadas sobre escalabilidad o ajuste de políticas de calidad de servicio (QoS).

Este módulo resulta esencial tanto para labores de diagnóstico como para asegurar el cumplimiento de los niveles de servicio esperados en la infraestructura de red, siendo una herramienta clave para administradores de sistemas en entornos corporativos a continuación vemos un ejemplo de la captura y monitoreo de tráfico desde. Endian Firewall.

Figura 9. Monitoreo de tráfico y desempeño del sistema



Fuente: Autoría Propia

6 GESTIÓN DE PAQUETES Y SOFTWARE

El software libre se basa en cuatro libertades esenciales: ejecutar el programa para cualquier propósito, estudiar cómo funciona y modificarlo, redistribuir copias, y distribuir versiones modificadas. Estas libertades están respaldadas por licencias como la GPL (General Public License) y la licencia MIT, que garantizan derechos a los usuarios finales y fomentan un ecosistema de colaboración y transparencia [1]. Esta filosofía no solo impulsa la innovación técnica, sino que también empodera a las comunidades educativas y profesionales a crear soluciones adaptadas a sus contextos específicos. El modelo de desarrollo abierto facilita auditorías de seguridad independientes, mejora continua del código y evita la dependencia de proveedores propietarios.

6.1 COMPARATIVA DE DISTRIBUCION

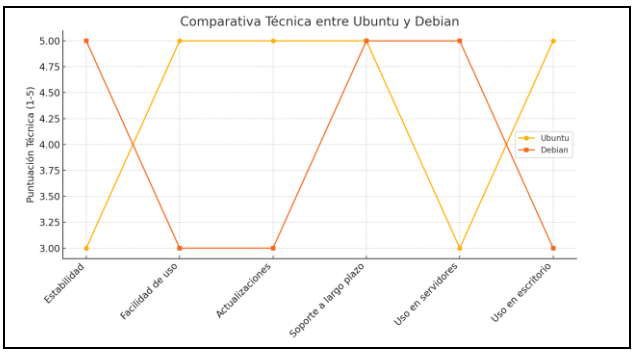
El ecosistema GNU/Linux, Debian y Ubuntu se posicionan como dos de las distribuciones más influyentes. Debian es conocida por su enfoque en la estabilidad, siendo la elección preferida en entornos de servidor y misiones críticas donde se requiere una base robusta y probada. Sus ciclos de lanzamiento son más prolongados, lo que minimiza interrupciones por cambios frecuentes y permite un mayor control sobre las actualizaciones [2].

Ubuntu, derivada directamente de Debian, adopta un enfoque más amigable para el usuario y más dinámico en cuanto a ciclos de desarrollo. Ofrece lanzamientos regulares, incluyendo versiones LTS (Long Term Support) con cinco años de soporte, lo cual la hace ideal para usuarios nuevos, estaciones de trabajo y servicios en la nube. Además, cuenta con una comunidad amplia, extensa documentación y compatibilidad con software comercial.

Ambas distribuciones utilizan herramientas comunes de gestión de paquetes como apt y dpkg, lo que permite instalar, actualizar y remover software de manera eficiente. Además, han adoptado tecnologías modernas de empaquetado como

Snap y Flatpak, que ofrecen portabilidad, entornos aislados y mayor control sobre las dependencias del software instalado [3]. La elección entre una u otra dependerá de los objetivos del entorno: estabilidad y control con Debian; usabilidad y flexibilidad con Ubuntu.Debian destaca por su estabilidad; Ubuntu, por su facilidad de uso y actualizaciones regulares. Ambas utilizan apt y dpkg, con soporte para Snap y Flatpak [3].

Figura 10. Comparativa visual entre Debian y Ubuntu



Fuente: Autoría Propia

La comparativa visual entre Debian y Ubuntu respecto a estabilidad, facilidad de uso, frecuencia de actualizaciones y soporte comunitario. La elección entre una u otra dependerá de los objetivos del entorno: estabilidad y control con Debian; usabilidad y flexibilidad con Ubuntu.Debian destaca por su estabilidad; Ubuntu, por su facilidad de uso y actualizaciones regulares [4]. Ambas utilizan apt y dpkg, con soporte para Snap y Flatpak [5].

7 ADMINISTRACIÓN DE USUARIOS Y SERVICIOS

La administración de usuarios y grupos es una función crítica en cualquier sistema operativo, especialmente en GNU/Linux, donde el control de acceso determina la seguridad y la eficiencia operativa. Permite establecer límites de acceso, delegar responsabilidades y fortalecer la protección de los recursos mediante políticas de contraseñas robustas, separación de privilegios y mecanismos de autenticación avanzados. La inclusión de autenticación centralizada mediante LDAP o Active Directory facilita la gestión de múltiples usuarios desde una ubicación centralizada, lo cual es vital en entornos corporativos [6]. Además, se recomienda la desactivación de cuentas inactivas, el uso de claves SSH en lugar de contraseñas y la implementación de autenticación de dos factores (2FA).

7.1 SERVICIOS DE RED GNU/LINUX

Permite desplegar y administrar una amplia gama de servicios de red esenciales para el funcionamiento de infraestructuras modernas. Esto incluye servidores DNS (como BIND9), servicios de correo electrónico con Postfix y Dovecot, así como servidores web como Apache y Nginx. El uso de interfaces de administración como phpMyAdmin facilita la interacción con bases de datos como MySQL. La seguridad en estos servicios se refuerza mediante el uso de TLS/SSL, firewalls como iptables o nftables, reglas de acceso restringidas, listas negras, autenticación segura y protección contra spam [7]. Asimismo, la integración con sistemas de monitoreo permite supervisar la disponibilidad y el rendimiento de estos servicios.

7.2 MÁQUINAS VIRTUALES Y CONTENEDORES

La virtualización y los contenedores son tecnologías clave en la consolidación de servicios y la creación de entornos de pruebas. Herramientas como VirtualBox y KVM permiten la creación de máquinas virtuales completas que replican entornos de hardware independientes. Por su parte, los contenedores con Docker ofrecen una solución ligera y flexible para ejecutar servicios aislados, facilitando el despliegue continuo y la portabilidad de aplicaciones. Estas tecnologías permiten realizar pruebas sin afectar el entorno de producción, implementar snapshots y gestionar recursos con gran eficiencia [4].

7.3 AUTOMATIZACIÓN DE TAREAS

La automatización es un pilar de la administración moderna. Utilidades como cron y systemd timers permiten programar tareas de mantenimiento, respaldos automáticos, limpieza de registros y ejecución periódica de scripts. Esto reduce la intervención manual, minimiza errores humanos y garantiza la consistencia operativa. Además, el uso de scripts bash personalizados permite encadenar procesos complejos en tareas rutinarias, mejorando la productividad del administrador del sistema

7.4 AUDITORÍA Y SEGURIDAD

La auditoría del sistema es indispensable para garantizar el cumplimiento normativo y la detección temprana de amenazas. GNU/Linux proporciona herramientas como logwatch para la generación de informes diarios, fail2ban para la detección y bloqueo de intentos de acceso no autorizados, y el uso de permisos extendidos (ACLs) para un control granular. La supervisión de archivos sensibles, el análisis de logs con rsyslog o journalctl, y la generación de alertas permiten una vigilancia continua del entorno. Estas prácticas son clave para mitigar riesgos, responder a incidentes y mantener la integridad del sistema.
Incluye registros de sistema, uso de permisos extendidos, herramientas como logwatch, fail2ban, y monitoreo de comportamientos sospechosos.

8 RESPALDO Y RECUPERACIÓN

8.1 RESPALDOS LOCALES Y REMOTOS

La estrategia de respaldo es un pilar esencial en la gestión de sistemas. Se recomienda seguir la regla 3-2-1: mantener al menos tres copias de los datos, almacenadas en dos medios diferentes y al menos una en una ubicación remota. Esta práctica protege contra pérdidas por fallos de hardware, errores humanos o ataques como ransomware.

Para respaldos locales, se utilizan herramientas como tar para comprimir archivos, y gpg para aplicar cifrado simétrico o asimétrico, garantizando la confidencialidad de los datos. rsync es ideal para sincronizar directorios de forma incremental, lo que ahorra tiempo y ancho de banda. En entornos remotos, scp y ssh permiten transferencias seguras entre servidores.

Además, es fundamental automatizar estos procesos mediante cron o systemd timers, asegurando su ejecución periódica. Las políticas de retención, la verificación de integridad de los respaldos y la restauración de prueba periódica son prácticas recomendadas para garantizar la efectividad del plan de recuperación.

8.2 DIAGNÓSTICO Y HERRAMIENTAS LIVE

En situaciones críticas, las distribuciones Live como Kali Linux, SystemRescue o Rescatux permiten el arranque del sistema sin necesidad de instalación, proporcionando acceso a herramientas de diagnóstico, recuperación de datos y análisis forense.

Entre las utilidades más destacadas se encuentran:
testdisk: para recuperar particiones perdidas o dañadas,
photorec: para restaurar archivos eliminados,
foremost: para análisis profundo de sectores del disco,
fsck: para verificar y reparar sistemas de archivos,
smartctl: para evaluar el estado físico del disco mediante la tecnología SMART.

Estas herramientas permiten enfrentar escenarios de corrupción de disco, pérdida de datos o errores del sistema de archivos de manera rápida y efectiva, minimizando el impacto en la operación.

8.3 MONITOREO DEL SISTEMA

El monitoreo continuo del sistema es crucial para detectar fallos anticipadamente y optimizar el rendimiento. Herramientas como logwatch generan resúmenes diarios de los eventos del sistema, facilitando la identificación de anomalías.

logrotate gestiona la rotación, compresión y eliminación de archivos de registro, evitando el consumo excesivo de espacio en disco. netdata ofrece dashboards interactivos con métricas en tiempo real, como uso de CPU, memoria, tráfico de red y operaciones de disco[8].

Plataformas más completas como Zabbix o Grafana, integradas con rsyslog, permiten recopilar, visualizar y analizar datos provenientes de múltiples nodos, generando alertas personalizadas y habilitando una gestión proactiva del estado del sistema.

La implementación de estas soluciones no solo mejora la visibilidad del entorno, sino que también refuerza la capacidad de respuesta ante incidentes y contribuye al mantenimiento de un alto nivel de disponibilidad del servicio.logwatch, logrotate, netdata, Zabbix, Grafana y rsyslog permiten consolidación de datos, alertas y visualización de métricas.[9]

9 CONCLUSIONES

- La integración de Endian Firewall Community (EFW) y GNU/Linux permite construir entornos informáticos caracterizados por su seguridad, eficiencia, escalabilidad y sostenibilidad. La implementación de políticas de seguridad perimetral mediante EFW ofrece una solución centralizada y robusta para la protección contra amenazas externas, facilitando además la segmentación de redes y el control granular del tráfico.

- El dominio de herramientas de administración en GNU/Linux —como bash, systemctl, apt, rsync, cron, entre otras— demuestra la importancia de contar con personal técnico capacitado para garantizar la continuidad operativa, automatización de tareas y reducción del margen de error humano.

- la adecuada gestión de servicios de red (DNS, correo, web, bases de datos), combinada con prácticas de monitoreo y auditoría, fortalece la infraestructura tecnológica frente a riesgos y fallos, asegurando alta disponibilidad y mejor tiempo de respuesta ante eventos adversos.

- La filosofía del software libre refuerza este enfoque al proporcionar transparencia, adaptabilidad y una comunidad activa que impulsa mejoras constantes. Distribuciones como Debian y Ubuntu permiten adaptar el sistema a distintos escenarios: desde servidores críticos hasta entornos de aprendizaje y desarrollo ágil.

- El uso de tecnologías de respaldo y recuperación, como la regla 3-2-1, junto con herramientas de monitoreo como Zabbix, Grafana y Netdata, consolidan la resiliencia del sistema frente a pérdidas de datos y caídas inesperadas. Además, los entornos virtualizados y la contenedorización facilitan el despliegue flexible y seguro de servicios.

En conjunto, estos elementos permiten establecer una infraestructura tecnológica autónoma, confiable y preparada para enfrentar los retos actuales de ciberseguridad y administración de TI. Adoptar buenas prácticas desde la instalación inicial hasta la operación cotidiana garantiza no solo la estabilidad del sistema, sino también la proyección a largo plazo de soluciones informáticas sostenibles.

REFERENCIAS

[1] Free Software Foundation. "*Software Libre y educación. El sistema operativo GNU",* 2016. [En línea]. Disponible en: http://www.gnu.org/education/education.html

[2] Canonical. "*Guía del Ubuntu desktop 20.04 LTS"*, 2023. [En línea]. Disponible en: https://help.ubuntu.com/20.04/ubuntu-help/index.html

[3] Debian. "*El manual del administrador de Debian 12.5.0"*, 2023. [En línea]. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html

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

[5] Guzmán, D. A., "*OVI Unidad I_Nivelacion, UNAD"*, 2017. [En línea]. Disponible en: http://hdl.handle.net/10596/10570
[6] Hernández, P. F., & Sánchez, J., "*Monitoreo y administración de sistemas Linux"*, UNAD, 2022. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/53211
[7] ISPConfig. [En línea]. Disponible en: https://www.ispconfig.org/?utm_source=chatgpt.com
[8] Red Hat. "*RHCSA Certification*." [En línea]. Disponible en: https://www.redhat.com/en/services/certification/rhcsa
[9] CompTIA. "*Linux+ Certification"*. [En línea]. Disponible en: https://www.comptia.org/certifications/linux
[10] Linux Foundation. "*Training"*. [En línea]. Disponible en: https://training.linuxfoundation.org/
.