

# Informe de Consultoría en Ciberseguridad para Emizin & Tech

## 1. Introducción

La empresa **Emizin & Tech** se dedica a la gestión y alojamiento de servicios en la nube para terceros, incluyendo páginas web, bases de datos, correo electrónico y máquinas virtuales. También cuenta con servicios internos (facturación, contabilidad, CRM) y presencia física a nivel nacional, con múltiples sucursales y una sede principal donde se aloja su **Data Center**.

Este informe tiene como objetivo **proponer una arquitectura de red segura y escalable** que permita proteger los activos digitales de Emizin & Tech frente a amenazas cibernéticas, garantizando la disponibilidad, confidencialidad e integridad de sus servicios.

---

## 2. Objetivo del informe

El objetivo es diseñar una **topología de red segura** que contemple:

- Comunicación segura entre sucursales.
  - Aislamiento entre servicios internos y públicos.
  - Separación de la red de invitados.
  - Aplicación de protocolos y herramientas modernas de ciberseguridad.
- 

## 3. Topología propuesta

### 3.1 A nivel nacional

- La sede principal (con Data Center) actuará como **hub central**.
- Las sucursales se conectan a la sede principal mediante **VPNs site-to-site usando WireGuard**.
- Esta arquitectura **hub-and-spoke** permite centralizar la administración y aplicar controles uniformes desde el núcleo.
- Todo el tráfico intersucursal será cifrado usando claves generadas por WireGuard, garantizando autenticación y confidencialidad.

### 3.2 A nivel local (sucursal principal)

- Se segmenta la red mediante **VLANs** para minimizar el riesgo lateral:
    - **VLAN 10**: Administración y dirección.
    - **VLAN 20**: Servicios internos (CRM, contabilidad, facturación).
    - **VLAN 30**: Red Wi-Fi de invitados, aislada completamente de los recursos internos.
    - **VLAN 40**: DMZ (Zona desmilitarizada) que alberga la web corporativa, el servidor DNS público y el correo externo.
  - El tráfico entre VLANs pasa por un **firewall de nueva generación (NGFW)** que inspecciona tráfico a nivel de aplicación y filtra según políticas definidas.
- 

## 4. Herramientas y protocolos de seguridad utilizados

- **WireGuard:** Solución VPN ligera y moderna para la conexión cifrada entre sedes.
  - **Firewall NGFW:** Con capacidades de inspección profunda (Deep Packet Inspection), detección de malware, filtrado geográfico y control por aplicación.
  - **IDS/IPS (como Suricata o Snort):** Para detectar intrusiones en tiempo real y actuar ante amenazas.
  - **WPA3:** Estándar de cifrado para Wi-Fi moderno, aplicado a redes internas e invitadas.
  - **HTTPS con TLS 1.3:** Para proteger todos los servicios web, tanto internos como públicos.
  - **Autenticación Multifactor (MFA):** Requisito para accesos administrativos o remotos.
  - **Gestor de parches:** Sistema de actualización automatizada para servicios críticos.
  - **SIEM (como Graylog o Wazuh):** Para centralizar logs y detectar correlaciones anómalas.
- 

## 5. Justificación técnica

- **La segmentación con VLANs** mejora el control interno y reduce la propagación de amenazas.
- La **DMZ** protege el núcleo interno al aislar servicios expuestos públicamente.
- **WireGuard** se elige por su seguridad, facilidad de configuración y bajo consumo de recursos.

- **MFA** asegura que incluso si las credenciales se ven comprometidas, no se puede acceder sin el segundo factor.
  - **SIEM e IDS/IPS** permiten detección proactiva de amenazas y rápida respuesta.
- 

## 6. Descripción de los mapas de red

### Mapa Nacional (hub-and-spoke):

- La sede principal se conecta con cada sucursal a través de **túneles VPN WireGuard**.
- Cada sucursal tiene acceso a los recursos del Data Center, pero no se conectan directamente entre sí (solo a través del hub).
- Todo el tráfico es cifrado punto a punto.

### Mapa Sede Principal:

- **Router de entrada** conectado al firewall NGFW.
- Switch gestionable L3 que distribuye el tráfico por VLAN:
  - VLAN 10, 20, 30 y 40.
- **Firewall inter-VLAN** define reglas específicas entre segmentos.
- Servidores internos (CRM, facturación) están aislados de la red pública.
- DMZ con servicios web públicos expuestos pero controlados.

---

## **7. Conclusión**


La topología propuesta responde a las necesidades de seguridad de Emizin & Tech con un diseño escalable, segmentado y basado en buenas prácticas. La infraestructura protege tanto los servicios propios como los que la empresa brinda a terceros, estableciendo una base sólida para el cumplimiento normativo y la continuidad de negocio.

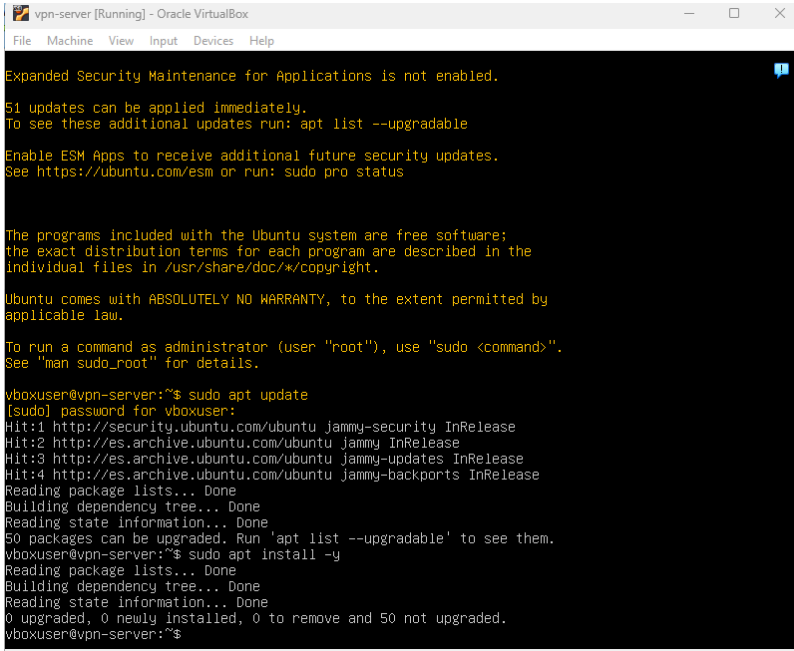
---

## **8. Recomendaciones adicionales**

- Realizar auditorías de seguridad y pruebas de penetración cada 6–12 meses.
  - Formar regularmente al personal en buenas prácticas de ciberseguridad.
  - Establecer un plan de respuesta ante incidentes (IRP).
  - Mantener un inventario actualizado de activos y configuraciones.
- 

## **9. Anexo técnico – Configuración de la VPN con WireGuard**

 **Figura 1.** Confirmación de que WireGuard ya estaba instalado en el servidor Ubuntu.



```
vpn-server [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Expanded Security Maintenance for Applications is not enabled.
51 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


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

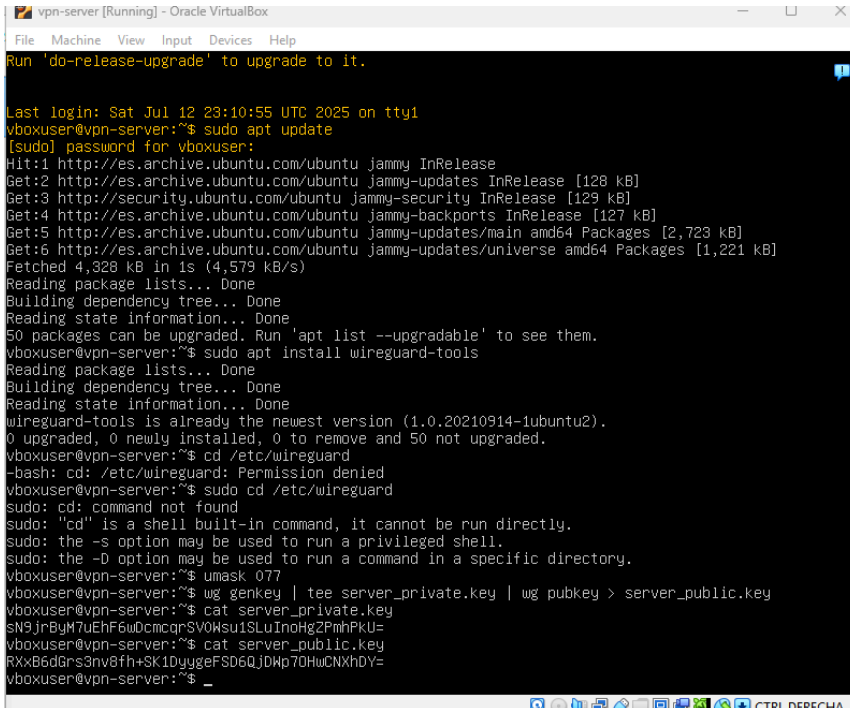
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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

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

vboxuser@vpn-server:~$ sudo apt update
[sudo] password for vboxuser:
Hit:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:2 http://es.archive.ubuntu.com/ubuntu jammy InRelease
Hit:3 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
50 packages can be upgraded. Run 'apt list --upgradable' to see them.
vboxuser@vpn-server:~$ sudo apt install -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 50 not upgraded.
vboxuser@vpn-server:~$
```

 **Figura 2.** Generación de claves pública y privada para WireGuard.

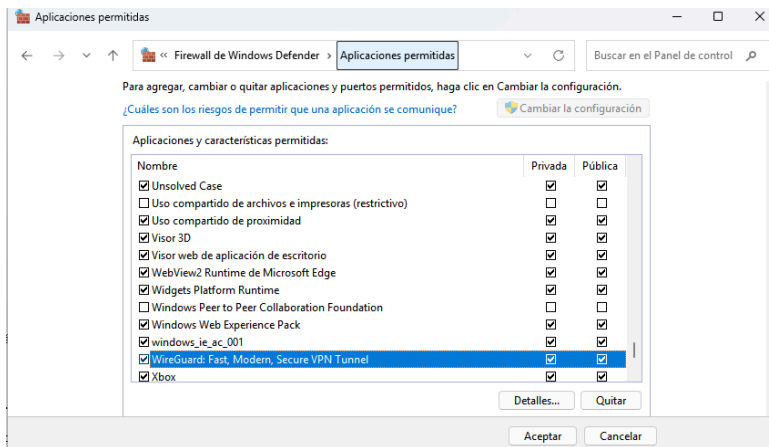


```
vpn-server [Running] - Oracle VirtualBox
File Machine View Input Devices Help

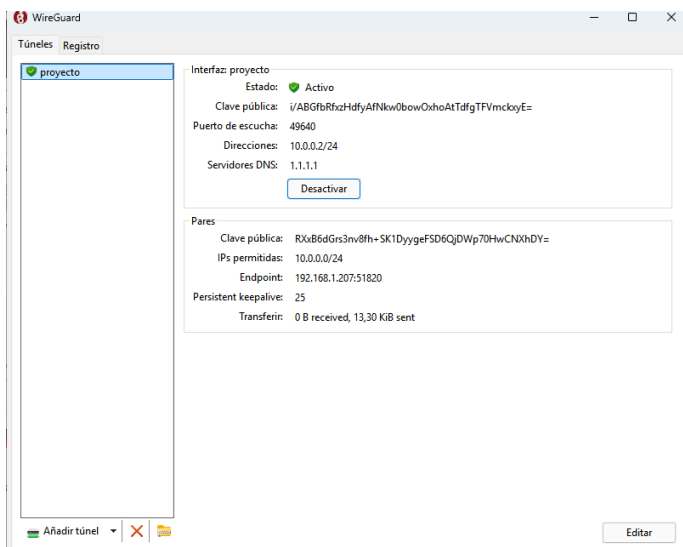
Run 'do-release-upgrade' to upgrade to it.


Last login: Sat Jul 12 23:10:55 UTC 2025 on tty1
vboxuser@vpn-server:~$ sudo apt update
[sudo] password for vboxuser:
Hit:1 http://es.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:4 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:5 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2,723 kB]
Get:6 http://es.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1,221 kB]
Fetched 4,328 kB in 1s (4,579 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
50 packages can be upgraded. Run 'apt list --upgradable' to see them.
vboxuser@vpn-server:~$ sudo apt install wireguard-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wireguard-tools is already the newest version (1.0.20210914-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 50 not upgraded.
vboxuser@vpn-server:~$ cd /etc/wireguard
-bash: cd: /etc/wireguard: Permission denied
vboxuser@vpn-server:~$ sudo cd /etc/wireguard
sudo: cd: command not found
sudo: "cd" is a shell built-in command, it cannot be run directly.
sudo: the -s option may be used to run a privileged shell.
sudo: the -D option may be used to run a command in a specific directory.
vboxuser@vpn-server:~$ umask 077
vboxuser@vpn-server:~$ wg genkey | tee server_private.key | wg pubkey > server_public.key
vboxuser@vpn-server:~$ cat server_private.key
sN9JrByM7uEhF6wDcmqqrSV0Wsu1SLuInoHgZPmhPkU=
vboxuser@vpn-server:~$ cat server_public.key
RXxB6dGrs3nv8fh+SK1DyygeFSd6QJDWp70HwCNXh0Y=
vboxuser@vpn-server:~$
```

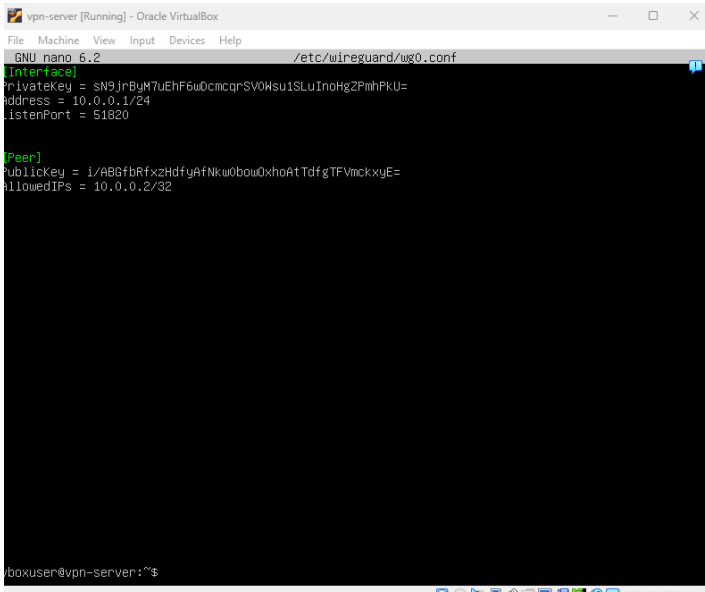
 **Figura 3.** Configuración del Firewall de Windows permitiendo la comunicación de la aplicación WireGuard.



**Figura 4.** Túnel activo en el cliente Windows, mostrando claves, endpoint y tráfico transmitido.




 **Figura 5.** Archivo *wg0.conf* del servidor Ubuntu con claves y parámetros definidos.

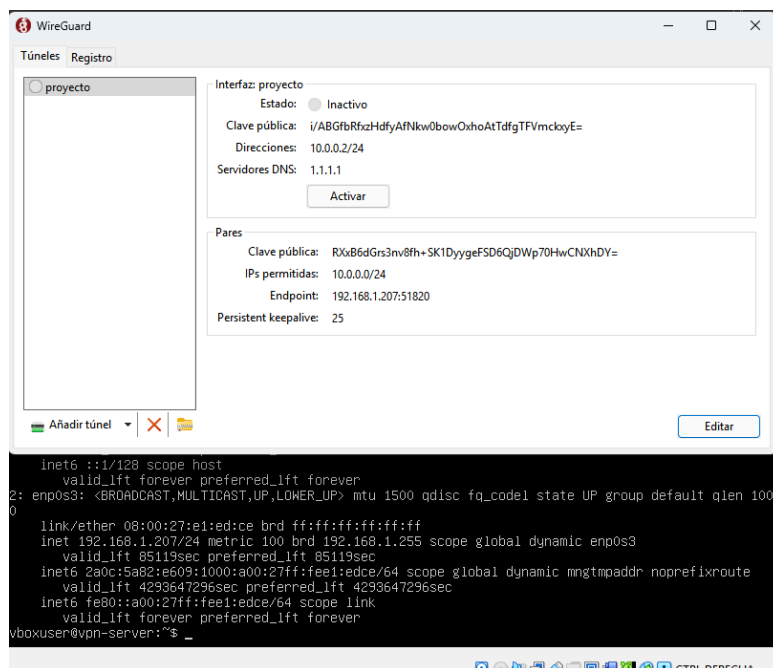


```
vpn-server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
GNU nano 6.2 /etc/wireguard/wg0.conf
[interface]
PrivateKey = sN9JnBjM7uEhF6u0cmqrSV0Hsu1SLuInoHgZPmhPkU=
Address = 10.0.0.1/24
ListenPort = 51820

[Peer]
PublicKey = i/ABGfbRfxzHdfyAfNkw0bowOxhoAtTdfgTFVmcKxyE=
AllowedIPs = 10.0.0.2/32

vboxuser@vpn-server:~$
```

 **Figura 6.** Configuración detallada del túnel WireGuard en el cliente Windows.



## Referencias



Cloud Security Alliance. (2019). *Security guidance for critical areas of focus in cloud computing* (v4.0). Cloud Security Alliance.

<https://cloudsecurityalliance.org/research/security-guidance/>

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, 4(2), 92–100. <https://doi.org/10.4236/jis.2013.42011>

Kshetri, N. (2017). Cloud computing in developing economies: Drivers, effects, and policy measures. In *Cloud Computing and Big Data* (pp. 3–21). Springer.

[https://doi.org/10.1007/978-3-319-59129-4\\_1](https://doi.org/10.1007/978-3-319-59129-4_1)