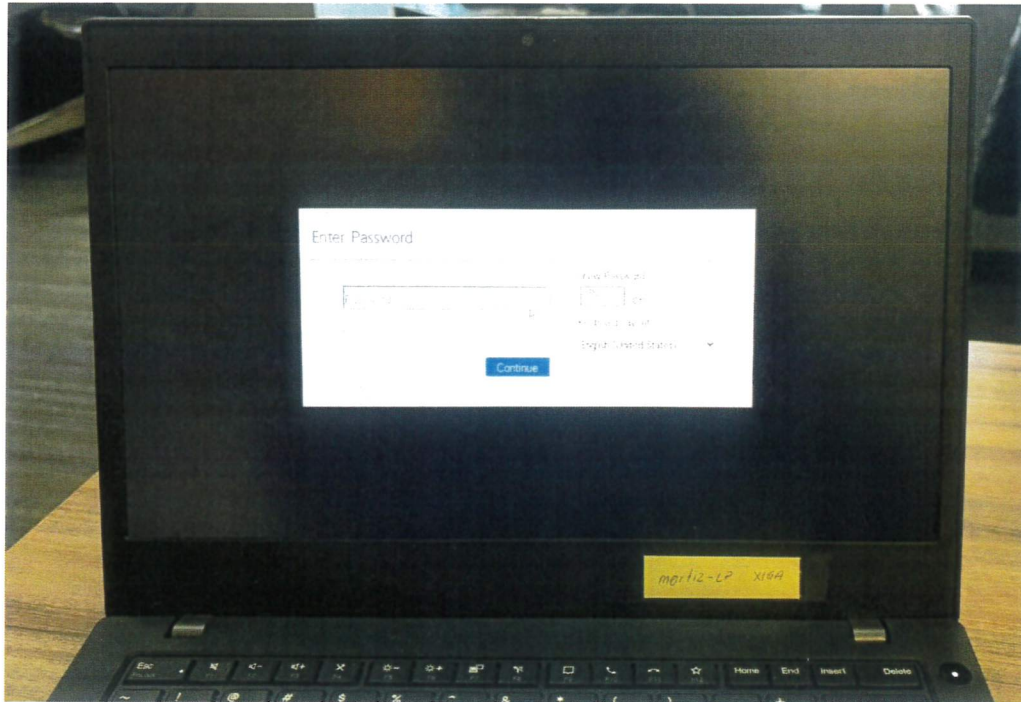


Req 48 - Evidencia de configuraciones de equipos de usuarios y servidores.

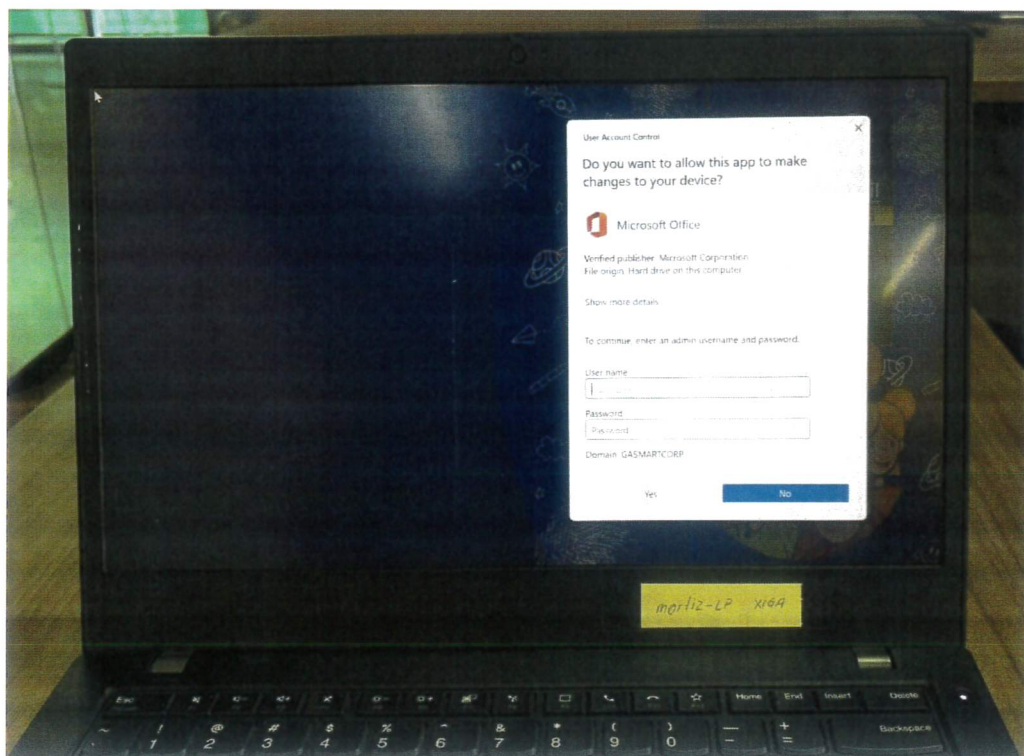
A) Para Equipos de empleados.

1. Evidencias de configuraciones de Activos para equipos de usuarios.

Inciso a) i. Ejemplo de protección de acceso al BIOS en equipos móviles.



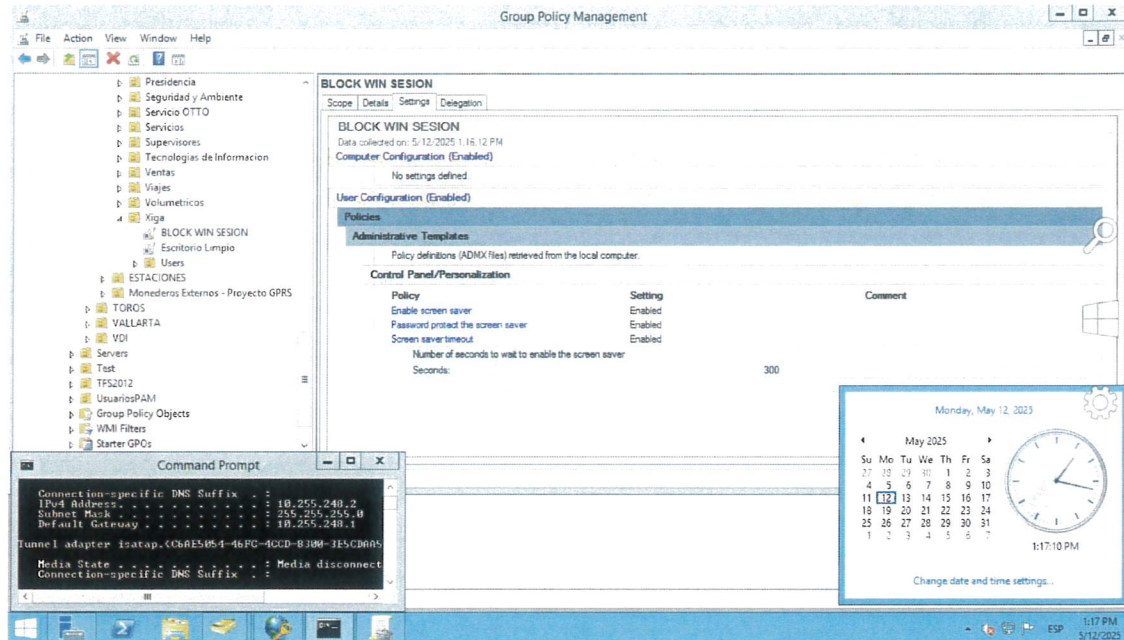
Inciso a) ii y iv Ejemplo de perfiles con restricción para hacer cambios de configuración.



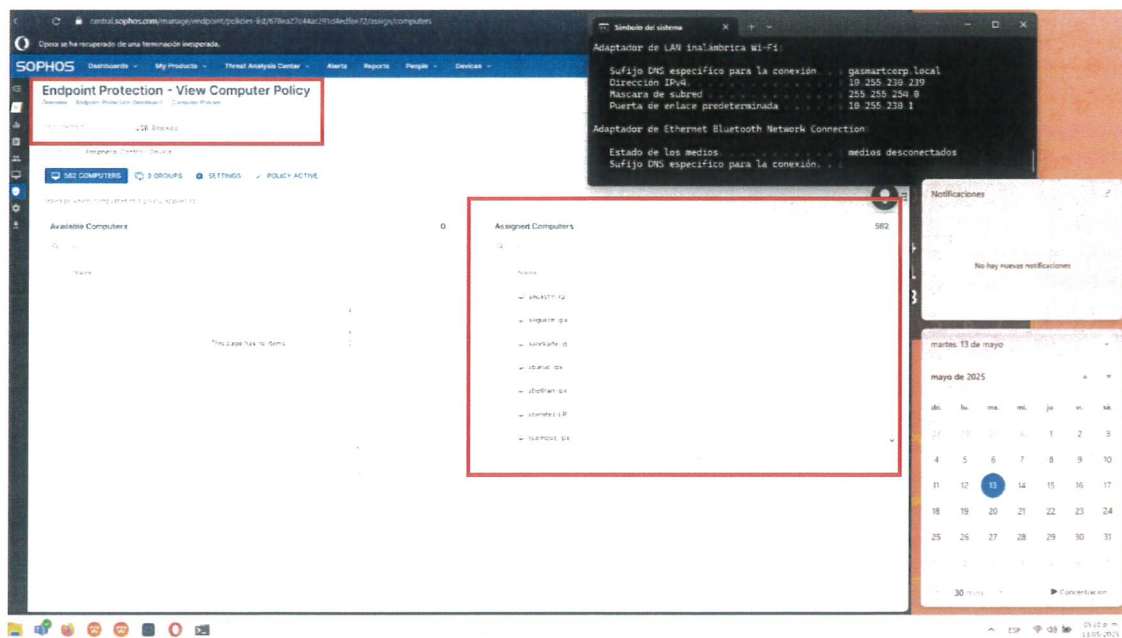
Handwritten signature

B) Para activos relacionados con las actividades del monedero electrónico

Inciso a) iii Limitación de derechos de acceso para modificación del s.o. Bloqueo de Pantalla por Política de AD.

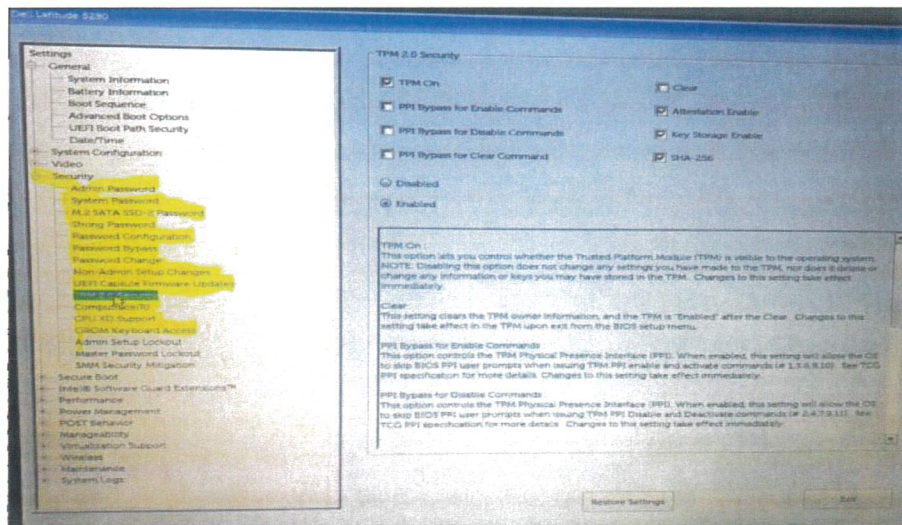


Inciso a) v Ejemplo de bloqueo de puertos USB en equipos de usuario con agente de antivirus.

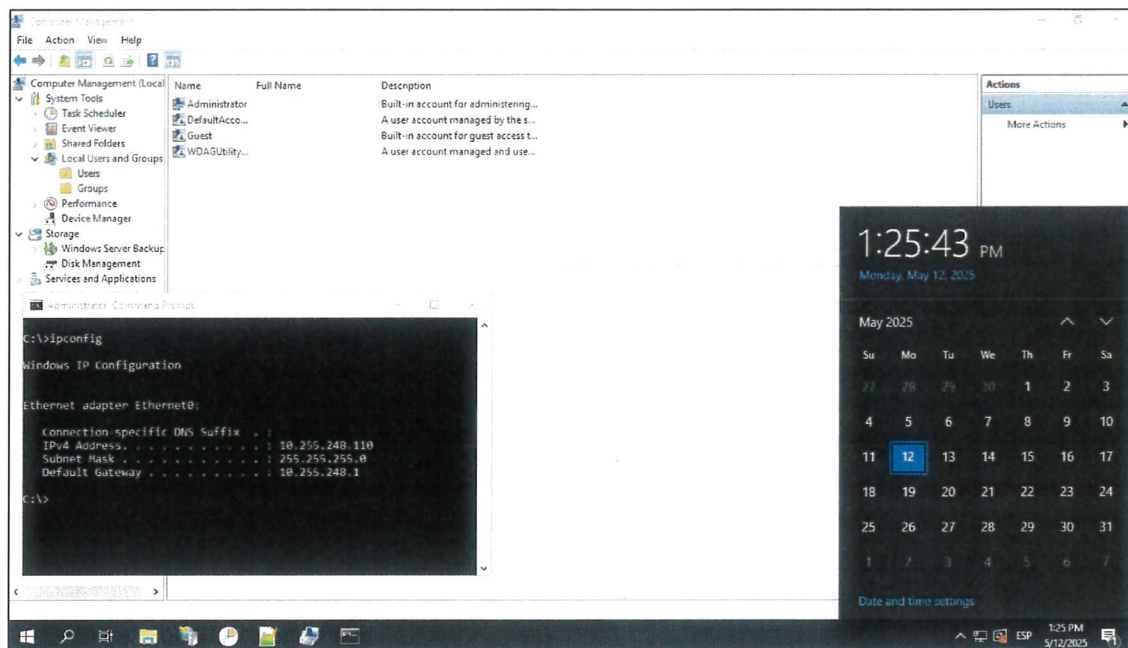


Handwritten signature

Inciso a) vi Configuraciones de Seguridad del Fabricante.



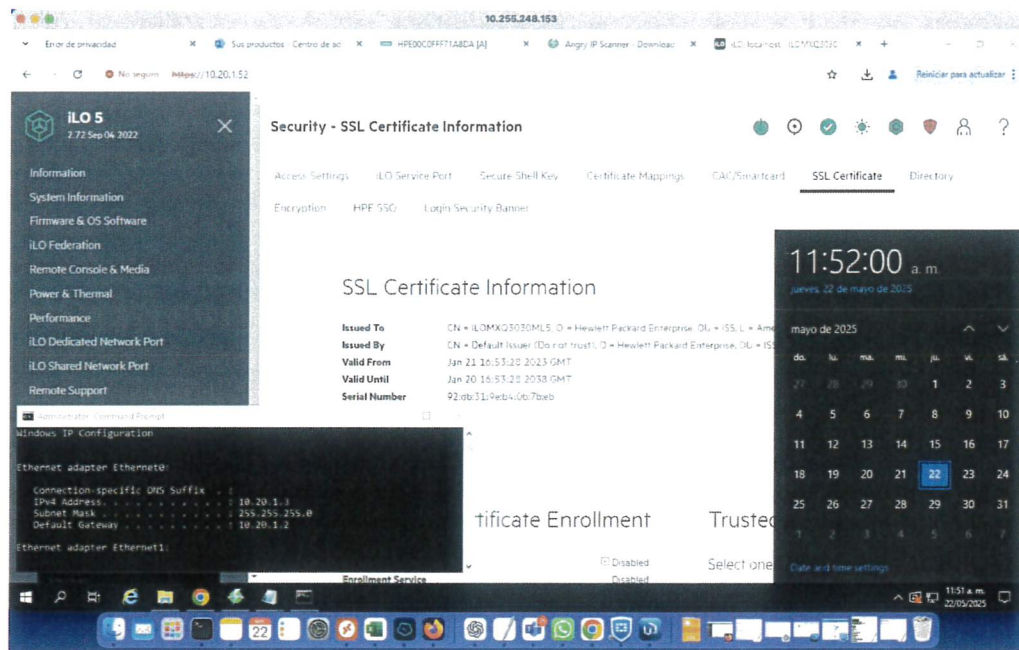
Inciso a) vii Usuarios por defecto deshabilitados en máquinas de usuarios.



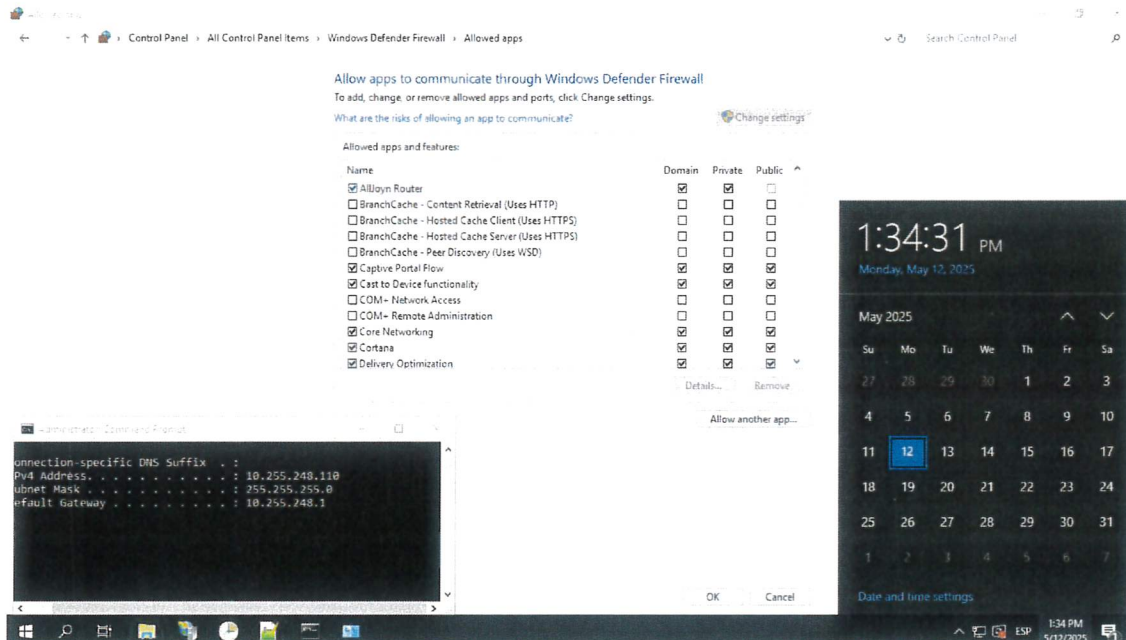
Handwritten signature

B) Evidencias de configuraciones de Activos relacionados con el monedero.inciso

b) i protección del BIOS

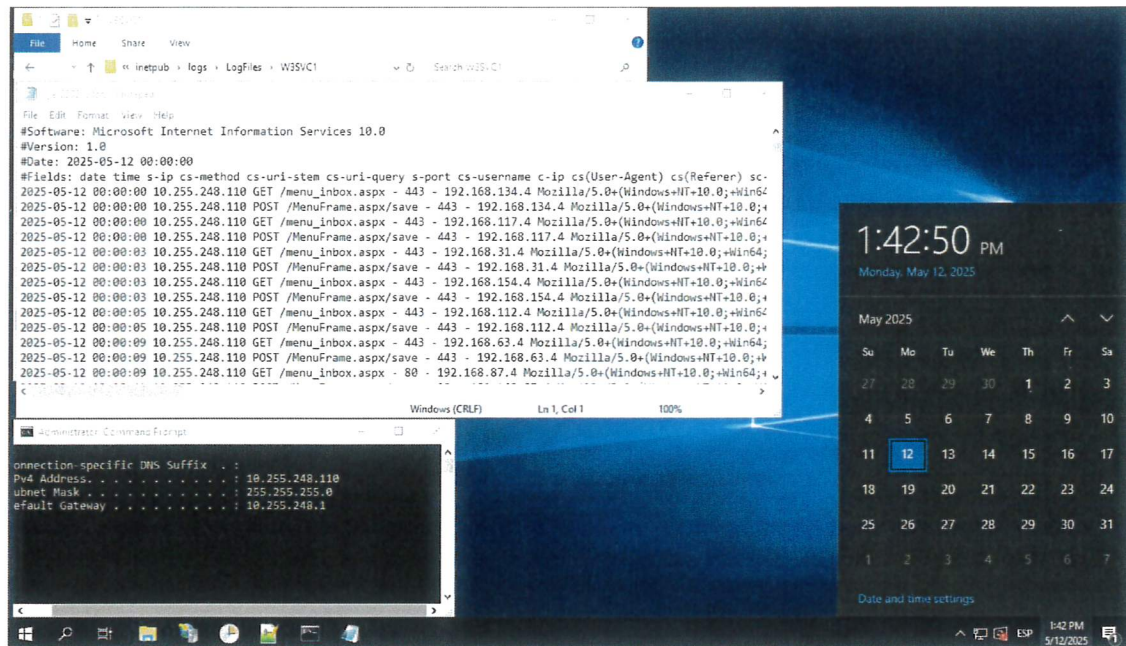


Inciso b) ii Configuración de puertos y protocolos.

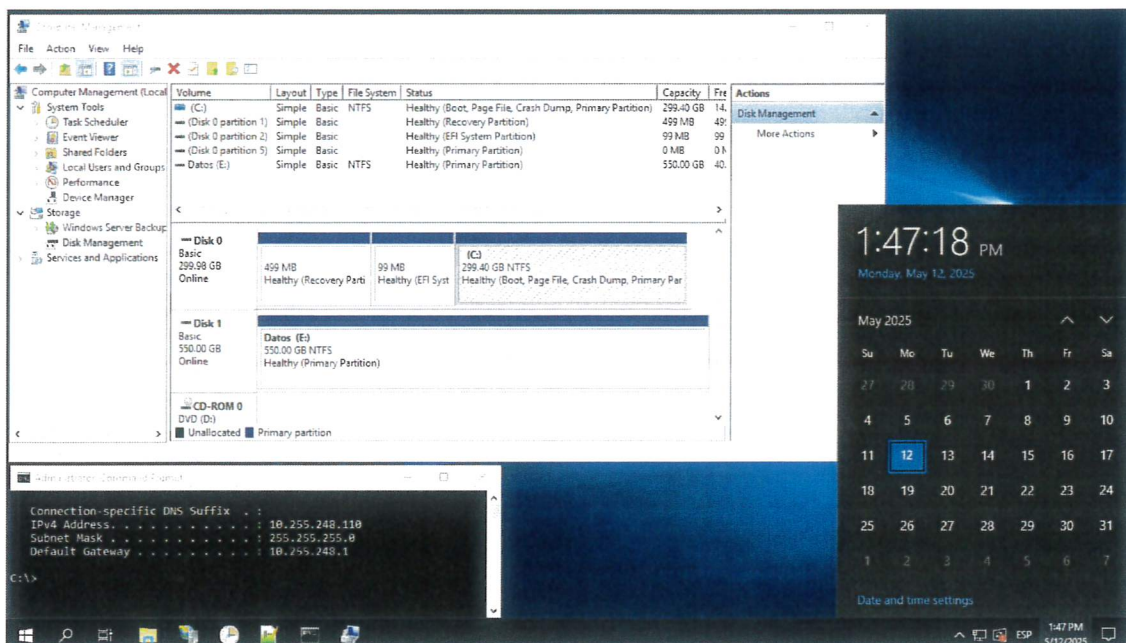


Handwritten signature

Inciso b) iii.Registro de actividades activado En sistema operativo y aplicaciones.



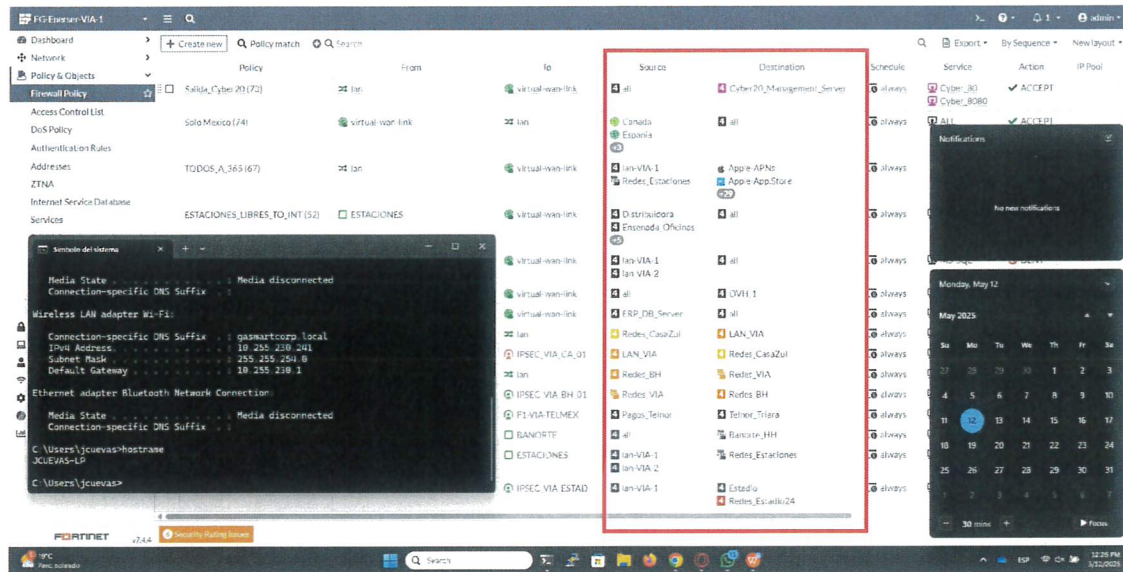
vi. Instalación de sistema operativo en partición exclusiva.



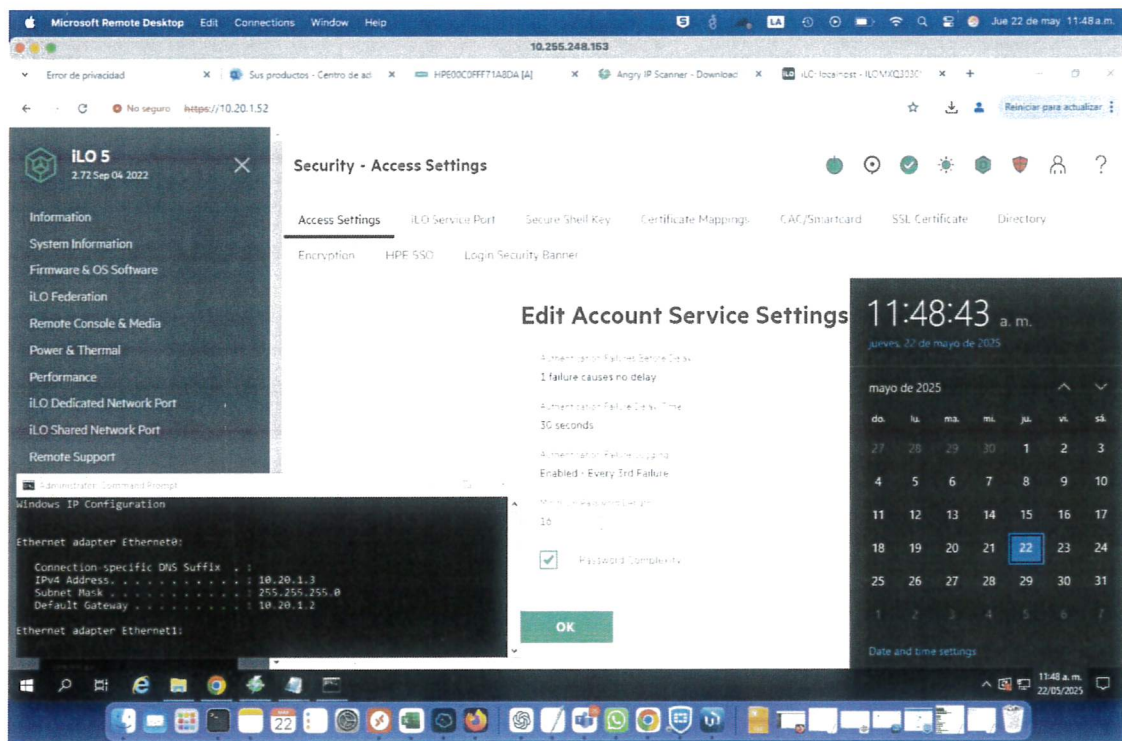
Handwritten signature

C) Para equipos de red

Inciso b) vii Reglas de filtrado de Paquetes.



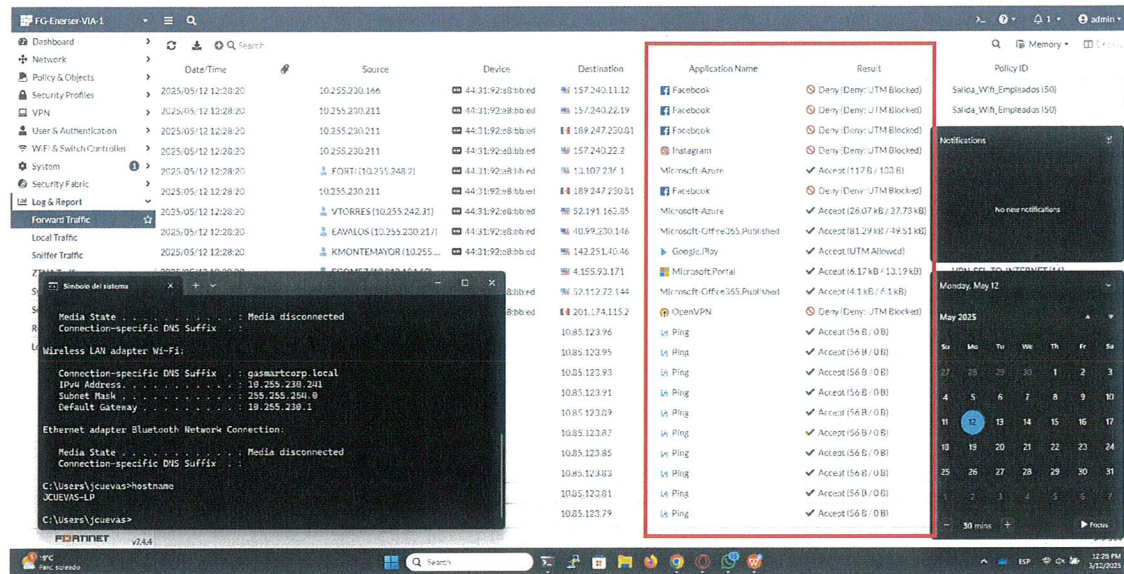
Inciso b) viii Configuraciones de Seguridad del Fabricante.



Desarrollado

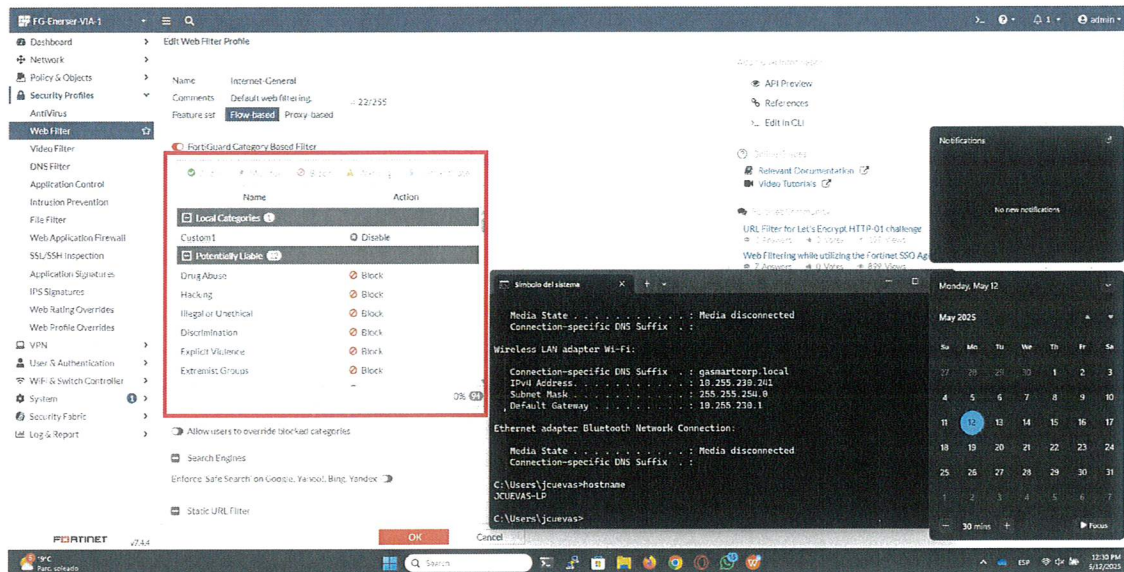
Evidencias de configuraciones para equipos de red

Inciso c) i Configuración de registro de actividades en equipos de red.



Date/Time	Source	Device	Destination	Application Name	Result
2025/05/12 12:28:20	10.255.230.166	44:31:92:8b:b0:ed	157.240.11.112	Facebook	Deny (Deny: UTM Blocked)
2025/05/12 12:28:20	10.255.230.211	44:31:92:8b:b0:ed	157.240.22.119	Facebook	Deny (Deny: UTM Blocked)
2025/05/12 12:28:20	10.255.230.211	44:31:92:8b:b0:ed	189.247.230.01	Facebook	Deny (Deny: UTM Blocked)
2025/05/12 12:28:20	10.255.230.211	44:31:92:8b:b0:ed	157.240.22.2	Instagram	Deny (Deny: UTM Blocked)
2025/05/12 12:28:20	FORTI (10.255.248.2)	44:31:92:8b:b0:ed	13.107.237.1	Microsoft Azure	Accept (117 B / 133 B)
2025/05/12 12:28:20	10.255.230.211	44:31:92:8b:b0:ed	189.247.230.01	Facebook	Deny (Deny: UTM Blocked)
2025/05/12 12:28:20	VITORRES (10.255.242.31)	44:31:92:8b:b0:ed	52.191.162.85	Microsoft Azure	Accept (26.07 KB / 27.73 KB)
2025/05/12 12:28:20	EAVILLOS (10.255.230.217)	44:31:92:8b:b0:ed	40.99.230.146	Microsoft Office365 Published	Accept (81.29 KB / 49.51 KB)
2025/05/12 12:28:20	KMONTEMAJOR (10.255.248.2)	44:31:92:8b:b0:ed	142.251.40.46	Google Play	Accept (UTM Allowed)
				Microsoft Portal	Accept (6.17 KB / 13.19 KB)
				Microsoft Office365 Published	Accept (4.1 KB / 1.4 KB)
				OpenVPN	Deny (Deny: UTM Blocked)
				is Ping	Accept (56 B / 0 B)
				is Ping	Accept (56 B / 0 B)
				is Ping	Accept (56 B / 0 B)
				is Ping	Accept (56 B / 0 B)
				is Ping	Accept (56 B / 0 B)
				is Ping	Accept (56 B / 0 B)
				is Ping	Accept (56 B / 0 B)
				is Ping	Accept (56 B / 0 B)
				is Ping	Accept (56 B / 0 B)

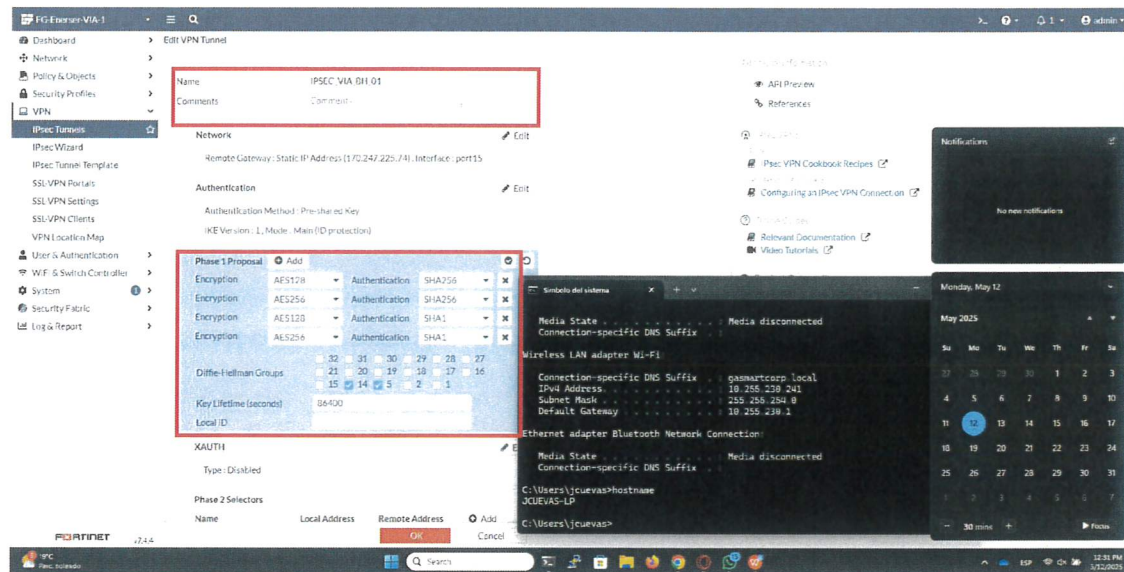
Inciso c) ii Configuración de política de firewall para bloqueo de sitios de alto riesgo



Name	Action
Local Categories	
Custom1	Disable
Potentially Liable	Block
Drug Abuse	Block
Hacking	Block
Illegal or Unethical	Block
Discrimination	Block
Explicit Violence	Block
Extremist Groups	Block

Handwritten signature

Inciso c) iii-1 Trafico de paquetes encriptado por VPN entre estaciones y el corporativo.

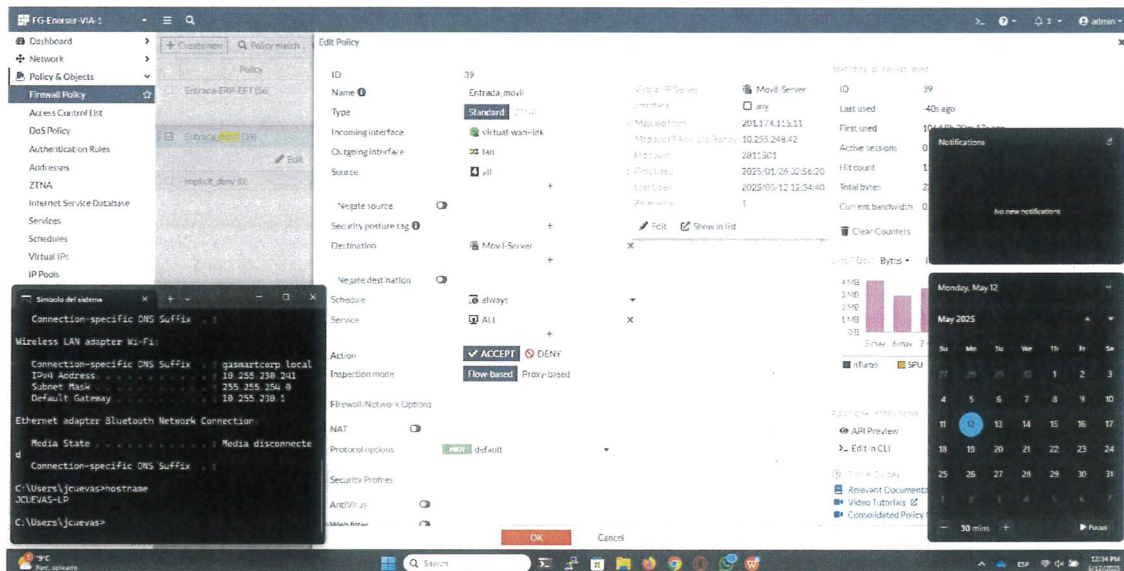


The screenshot shows the Fortinet FortiGate GUI for configuring a VPN Tunnel. The main configuration area is titled 'Edit VPN Tunnel' and shows the following settings:

- Name:** IPsec VIA DH 01
- Comments:** Comment
- Network:** Remote Gateway: Static IP Address (170.247.225.74), Interface: port15
- Authentication:** Authentication Method: Pre-shared Key, IKE Version: 1, Mode: Main (ID protection)
- Phase 1 Proposal:**
 - Encryption: AES128, Authentication: SHA256
 - Encryption: AES256, Authentication: SHA256
 - Encryption: AES128, Authentication: SHA1
 - Encryption: AES256, Authentication: SHA1
 - Diffie-Hellman Groups: 32, 31, 30, 29, 28, 27, 26, 25, 24, 23, 22, 21, 20, 19, 18, 17, 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1
 - Key Lifetime (seconds): 86400
 - Local ID: [empty]
- XAUTH:** Type: Disabled
- Phase 2 Selectors:** Name, Local Address, Remote Address, Add, Cancel

A terminal window in the bottom right shows the command 'show vpn tunnel' output, which includes details about the tunnel's status, connection-specific DNS suffix, and IP addresses.

Inciso c) iii-2 Servicios expuestos a Internet a través del Firewall que solo permita los puertos necesarios.



The screenshot shows the Fortinet FortiGate GUI for configuring a Firewall Policy. The main configuration area is titled 'Edit Policy' and shows the following settings:

- ID:** 39
- Name:** Entrada móvil
- Type:** Standard
- Incoming interface:** virtual-wan-link
- Outgoing interface:** lan
- Source:** all
- Negate source:** [checked]
- Security posture tag:** [empty]
- Destination:** Movil-Server
- Negate destination:** [checked]
- Schedule:** always
- Service:** All
- Action:** ACCEPT
- Inspection mode:** Proxy-based
- Firewall Network Options:** NAT, Protocol options, Security Profiles, AntiVirus

A terminal window in the bottom left shows the command 'show firewall policy' output, which includes details about the policy's status, schedule, and action.

Handwritten signature

Inciso c) iii-3 Trafico proveniente de internet analizado por IPS e IDS, Antivirus, etc.

The screenshot displays the Fortinet FortiGate configuration interface. The left sidebar shows the navigation menu with 'Intrusion Prevention' selected. The main panel shows the 'IPS Signatures and Filters' configuration page. A red box highlights the 'Create New' button and the list of signatures. The table below shows the list of signatures and their status.

Signature Name	Exempt IPs	Action	Packet Logging
IIISetminISMDLLAccess	0	Default	Disabled
IIISamplesISSamplesAccess	0	Default	Disabled
MSIISASPDLLHTMLEncodersBufferOverflow	0	Default	Disabled
MSIISBitmarkBigTalkHttpReceiveAccess	0	Default	Disabled
MSIISClientExceedingHeapBufferOverflow	0	Default	Disabled
MSIISChunkedEncodingTransferBufferOverflow	0	Default	Disabled
MSIISCommandShellSQLInjection	0	Default	Disabled
MSIISConfigurationFileInformationDisclosure	0	Default	Disabled
MSIISCpuJunkDLLAccess	0	Default	Disabled

Below the table, there is a 'Botnet C&C' section with a 'Scan Outgoing Connections to Botnet Sites' button. A terminal window in the foreground shows network configuration details for a wireless LAN adapter.

```

Simulo del sistema
Connection-specific DNS Suffix :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix : gasmartcorp.local
IPv4 Address . . . . . : 10.255.230.201
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 10.255.230.1
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnecte
Connection-specific DNS Suffix :
C:\Users\jcuevas>ipconfig
C:\Users\jcuevas>
  
```

Handwritten signature

Inciso c) iv Segregación de Redes

```

switch-mode normal chassis 2 slot 4
switch-mode normal chassis 2 slot 5
switch-mode normal chassis 2 slot 7
#
interface enable
switch-mode route-normal
#
password-recovery enable
#
vlan 1
#
vlan 2
description Network Management
name Network Management
#
vlan 3
name Estáticos
#
vlan 5
name Invitados
#
vlan 6
name Ilo
#
vlan 8
name Telefonía
#
vlan 9
name Sistemas
#
vlan 10
name Usuarios
#
vlan 11
name Servidores
#
vlan 13
name CCTV
#
vlan 14
name Control de Acceso
#
vlan 15
name VOI
#
vlan 16
name Wifi Guest
#
vlan 17
name Internet
#
vlan 18
name Segmenta 200

```

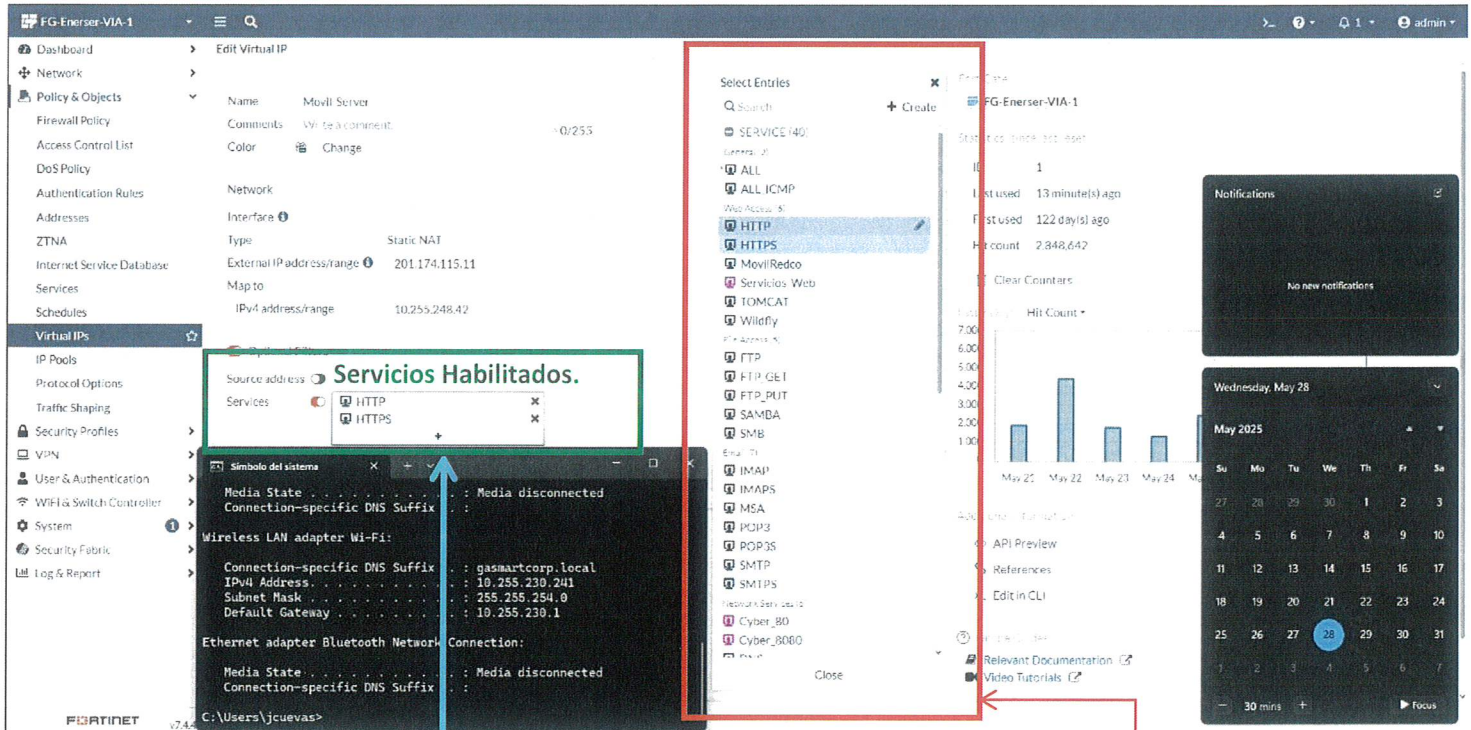
```

dhcp select relay
dhcp relay server-select 2
#
interface Vlan-Interface3
ip address 10.255.242.2 255.255.255.0
#
interface Vlan-Interface5
ip address 10.255.240.2 255.255.255.0
dhcp select relay
dhcp relay server-select 2
#
interface Vlan-Interface6
ip address 10.255.248.1 255.255.255.0
#
interface Vlan-Interface7
ip address 10.255.244.1 255.255.255.0
dhcp select relay
dhcp relay server-select 2
#
interface Vlan-Interface8
ip address 10.255.240.1 255.255.255.0
dhcp select relay
dhcp relay server-select 2
#
interface Vlan-Interface11
ip address 10.255.248.1 255.255.255.0
dhcp select relay
dhcp relay server-select 2
#
interface Vlan-Interface13
ip address 10.255.248.2 255.255.255.0
dhcp select relay
dhcp relay server-select 2
#
interface Vlan-Interface14
ip address 10.255.242.1 255.255.255.0
dhcp select relay
dhcp relay server-select 2
#
interface Vlan-Interface15
ip address 10.255.248.3 255.255.255.0
dhcp select relay
dhcp relay server-select 2
#
interface Vlan-Interface16
ip address 10.255.244.2 255.255.255.0
dhcp select relay
dhcp relay server-select 2

```

Handwritten signature

iv) Inhabilitación de puertos físicos utilizados en transferencia de información o almacenamiento (salvo autorización formal).



The screenshot displays the Fortinet FG-Eraser-VIA-1 interface. On the left, the 'Virtual IPs' section is expanded, showing a 'Movil Server' configuration. A green box highlights the 'Servicios Habilitados' (Enabled Services) section, which lists 'HTTP' and 'HTTPS'. A blue arrow points from this box to a text box below. On the right, a 'Select Entries' dialog box is open, showing a list of protocols. A red box highlights this dialog, and a red arrow points from it to a text box below. The dialog lists various protocols, including 'SERVICE (40)', 'ALL', 'ALL ICMP', 'Web Access', 'HTTP', 'HTTPS', 'MovilRedco', 'Servicios Web', 'TOMCAT', 'Wierfly', 'FTP', 'FTP GET', 'FTP PUT', 'SMB', 'IMAP', 'IMAPS', 'MSA', 'POP3', 'POP3S', 'SMTP', 'SMTPS', 'Cyber_80', and 'Cyber_8080'. A bar chart and a calendar are also visible in the background.

Se muestran los servicios que se encuentran habilitados, por lo que se considera que todo aquel servicio no incluido en esta configuración se encuentra deshabilitado.

Protocolos Inhabilitados

Este listado muestra todos los protocolos que **NO** se encuentran configurados, para la operación del monedero.

Handwritten signature