



4.4.- SDN QinQ.

¿Qué es una VLAN Queue in Queue?

Queue in Queue

QinQ (conocido como apilamiento VLAN) está estandarizado por el IEEE 802.1ad. Encapsula la etiqueta VLAN con dos capas: una etiqueta interior (de una red privada) y una etiqueta exterior (de la red pública) que en nuestro caso hemos llamado datos un paquete etiquetado 802.11Q se encapsula en otra etiqueta 802.1Q.

los paquetes se reenvían en función de la etiqueta VLAN exterior en la red pública, se interpreta que la etiqueta forma parte de los datos, por lo que esta también se transmite en la red pública.

Al llegar a destino se “desgrana” transmitiendo el paquete en la red destino con la etiqueta original (voz)

Trama Ethernet con VLAN (voz)

Dirección Origen	Dirección Destino	Tag	Tipo de trama	Datos (46-1500)	Frame Check Sequence (FCS/CRC)
------------------	-------------------	-----	---------------	-----------------	--------------------------------

Trama Ethernet con VLAN (datos)

Dirección Origen	Dirección Destino	TPID	Tag	Tipo de trama	Datos (46-1500)	Frame Check Sequence (FCS/CRC)
------------------	-------------------	------	-----	---------------	-----------------	--------------------------------

Dirección Origen	Dirección Destino	TPID	Tag	TPID	Tag	Tipo de trama	Datos (46-1500)	Frame Check Sequence (FCS/CRC)
------------------	-------------------	------	-----	------	-----	---------------	-----------------	--------------------------------



Eduardo Taboada (Tecnocratica.net) · VLAN Queue in Queue (Todos los derechos reservados)

La tunelización Q-in-Q en VLAN permiten crear una conexión Ethernet de capa 2 entre dos extremos y dentro del tunel podemos tener otras 4096 VLAN, es decir, lo que estamos haciendo es meter una VLAN dentro de otra VLAN.



Queue in Queue

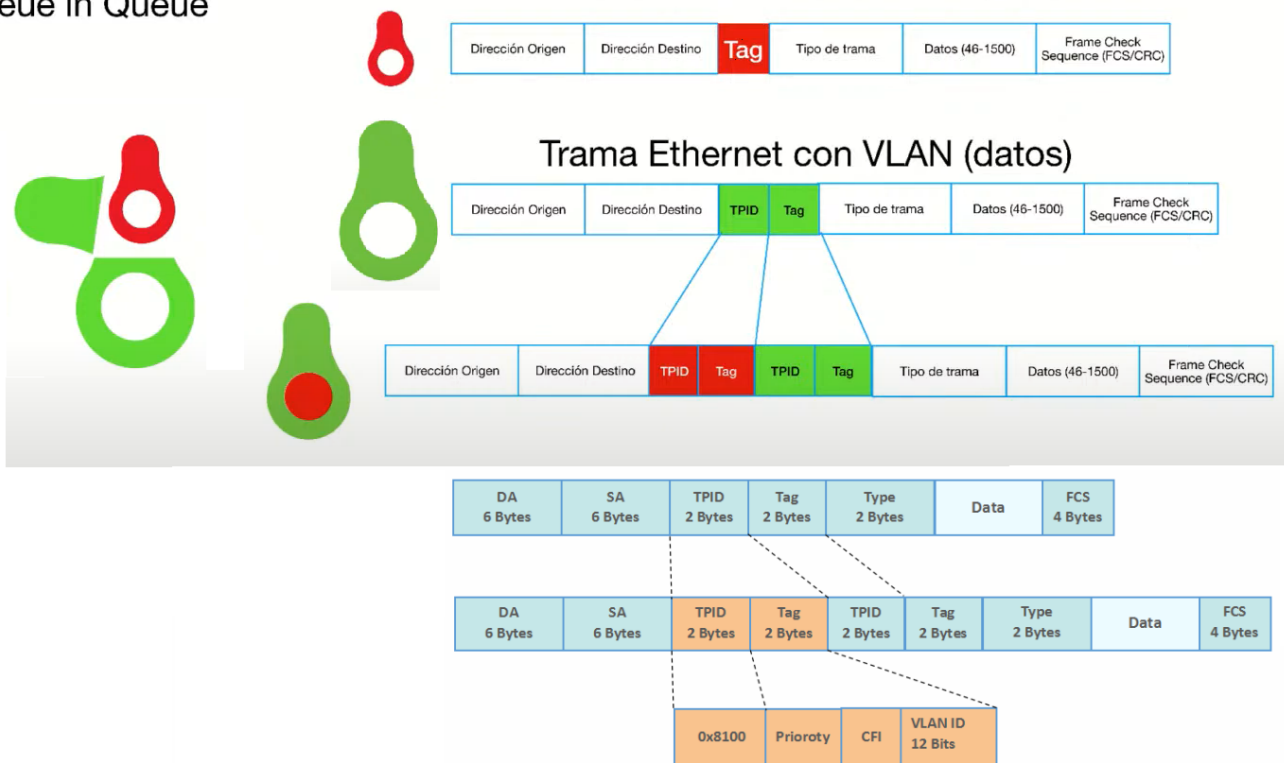


Imagen de elaboración propia: *Tunel QinQ de capa 2 y dentro una trama de VLAN de capa 2* ([CC BY-NC-SA](#))

Q-in-Q está estandarizado por el IEEE 802.1ad. Encapsula la etiqueta VLAN con dos capas: una etiqueta interior (de una red privada) y una etiqueta exterior (de la red pública). El etiquetado VLAN tradicional que utiliza el IEEE 802.1Q es incapaz de identificar y aislar los datos de los usuarios en las tramas crecientes de Ethernet. La tecnología QinQ se utiliza para ampliar la cantidad VLANs hasta **4096×4096**, de este modo se podrán ahorrar ID de VLAN.

Los paquetes QinQ tienen un formato fijo. Normalmente, un paquete etiquetado 802.11Q se encapsula en otra etiqueta 802.1Q, de la que deriva el nombre «Q-in-Q». Durante la transmisión, los paquetes se reenvían en función de la etiqueta VLAN exterior en la red pública, se interpreta que la etiqueta forma parte de los datos, por lo que esta también se transmite en la red pública. Como contienen esta forma de doble etiqueta, los paquetes QinQ tienen 4 bytes más que los paquetes comunes con etiqueta VLAN 802.1Q.

Reduce la MTU en los vínculos de acceso en al menos 4 bytes para que las tramas no excedan la MTU del enlace de troncalización cuando se agreguen las etiquetas VLAN.



QinQ

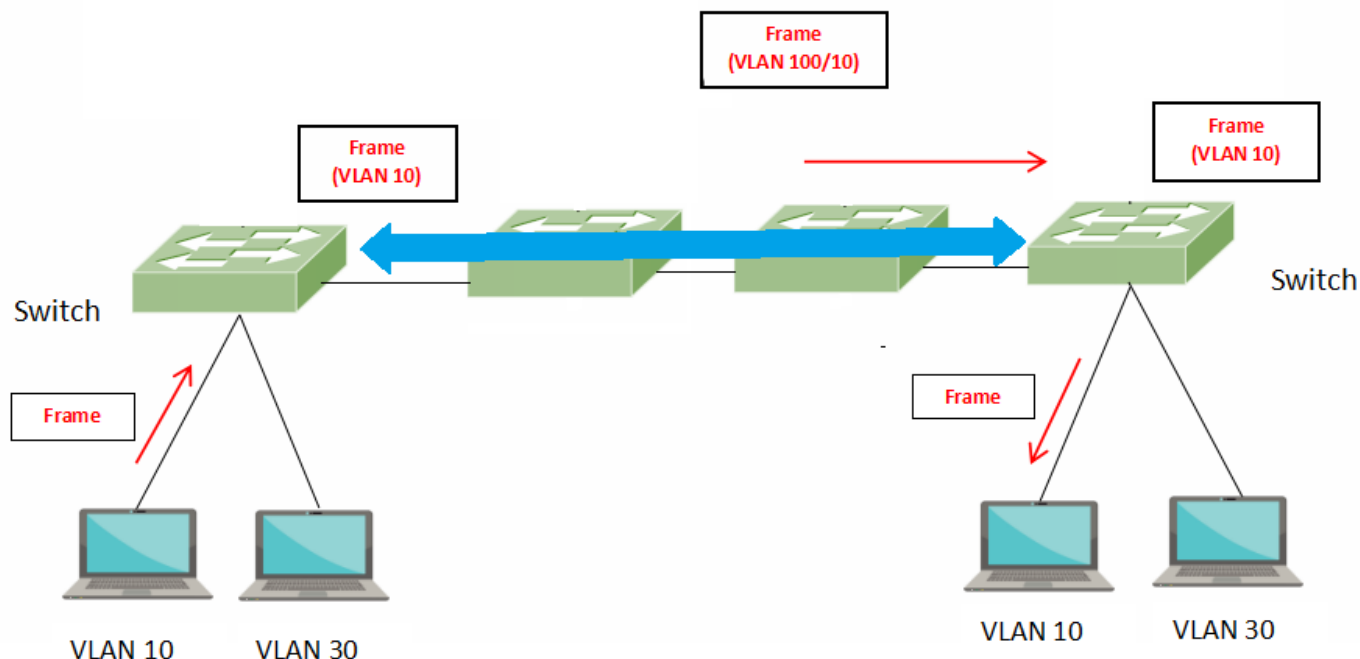


Imagen de elaboración propia· Esquema de tunelización QinQ de VLAN (CC BY-NC-SA)

Implementación de una Zona de SDN del tipo QinQ

Un caso de uso típico para esta configuración es un proveedor de hosting que proporciona una red aislada a los clientes para la comunicación de VM pero aísla las VM de otros clientes. Con QinQ cada cliente podría tener su propia VLAN (máximo de clientes 4096) pero para cada cliente se le podría proporcionar 4096 VLAN propias dentro de su tunel y aislar a su vez su tráfico de red.

Para el primer nodo Proxmox, crea una zona QinQ llamada "Qinq100" con el servicio VLAN 100 (que será la VLAN que vean todos los switch):



The screenshot shows the Proxmox VE 8.2.2 web interface. On the left, the 'Centro de datos' sidebar lists various resources. The main panel shows the 'Agregar: QinQ' dialog box. The dialog contains the following fields:

- ID: Qinq100
- Bridge: vmbro
- Servicio VLAN: 100
- Protocolo del Servicio VLAN: 802.1ad
- MTU: auto
- Nodos: Todo (Sin restricción)
- IPAM: pve
- Servidor de DNS: (empty)
- Servidor de DNS inverso: (empty)
- Zona de DNS: (empty)

At the bottom of the dialog, there is an 'Ayuda' button, a checked 'Avanzado' checkbox, and an 'Agregar' button.

Imagen de elaboración propia: *Creación de la Zona SDN tipo QinQ* ([CC BY-NC-SA](#))

Crea una VNet denominada "SQ10010" con VLAN-ID 10 en la zona "QinqZona100" creada anteriormente.



Centro de datos

- Dos factores
- Grupos
- Conjuntos
- Roles
- Dominios
- HA
- SDN
- Zonas
- VNets**
- Opciones
- IPAM
- ACME
- Cortafuego
- Servidor de Métricas
- Mapeo de recursos
- Notificaciones

VNets

Crear Eliminar Editar

ID ↑	Alias	Zona	Etiqueta	Consci...	Estado
------	-------	------	----------	-----------	--------

Crear: VNet

Nombre:

Alias:

Zona:

Etiqueta:

Consciente de VLAN: ☐


[Ayuda](#) [Crear](#)


Imagen de elaboración propia: Creación de la VNet SQ10010 con etiqueta VLAN 10 perteneciente a la Zona Qinq 100 ([CC BY-NC-SA](#))


Crea una VNet denominada "SQ10030" con VLAN-ID 30 en la zona "QinqZona100" creada anteriormente.





Centro de datos


 Dos factores


 Grupos


 Conjuntos


 Roles


 Dominios


 HA


 SDN


 Zonas


 **VNets**


 Opciones


 IPAM


 ACME

 Cortafuego

 Servidor de Métricas


 Mapeo de recursos

 Notificaciones

 Soporte

VNets

CrearEliminarEditar

ID ↑	Alias	Zona	Etiqueta	Consci...	Estado
SQ10010	Switch...	Qinq100	10		 new

Crear: VNet

Nombre:

SQ10030

Alias:

Switch VLAN30 encapsulado QinQ :

Zona:


Qinq100

Etiqueta:

30

Consciente de VLAN:

☐

 Ayuda

Crear

Imagen de elaboración propia: Creación VNet SQ10030 con etiqueta VLAN 30 encapsulado en QinQ 100 ([CC BY-NC-SA](#))

Crea una zona QinQ llamada "Qinq200" con el servicio VLAN 200 (que será para otro cliente):



Agregar: QinQ

ID:

Qinq200

Bridge:

vmbr0

Servicio VLAN:

200

Protocolo del Servicio VLAN:

802.1ad

MTU:

auto

Nodos:

Todo (Sin restricción)

IPAM:

pve

Servidor de DNS:

Servidor de DNS inverso:

Zona de DNS:

Ayuda

Avanzado ☒

Agregar

Imagen de elaboración propia: Creación de otra Zona QinQ para comprobar el aislamiento del tráfico Ethernet ([CC BY-NC-SA](#))

Crea una VNet denominada "SQ20010" con VLAN-ID 10 en la zona "Qinq200" creada anteriormente.

Crea una VNet denominada "SQ20030" con VLAN-ID 30 en la zona "Qinq200" creada anteriormente.

Aplica la configuración en SDN y repetir en mismo proceso en el nodo 2 de Proxmox.



PROXMOX Virtual Environment 8.2.2

Vista por servidor

Centro de datos

- vm-proxmox-c01
 - 100 (LXC-Ubuntu23.04-01)
 - Qinq100 (vm-proxmox-c01)
 - Qinq200 (vm-proxmox-c01)
 - localnetwork (vm-proxmox-c01)
 - NFS-Compartido-ISO (vm-proxmox-c01)
 - local (vm-proxmox-c01)
 - local-lvm (vm-proxmox-c01)
 - Pool_ASIR1_alum1
 - Pool_ASIR1_alum2
 - Pool_PROF_profe1
 - Pool_PROF_profe2
 - Pool_TIC_alum3
 - Pool_TIC_alum4

Centro de datos

- Dos factores
- Grupos
- Conjuntos
- Roles
- Dominios
- HA
- SDN
- Zonas
- VNets**
- Opciones
- IPAM

VNets

ID ↑	Alias	Zona	Etiqueta	Consci...	Estado
SQ10010	Switch...	Qinq100	10		
SQ10030	Switch...	Qinq100	30		
SQ20010		Qinq200	10		
SQ20030		Qinq200	30		

Imagen de elaboración propia: Aplicar cambios en la SDN para crear toda la configuración de red (CC BY-NC-SA)

← → ↻ No es seguro | <https://192.168.30.119:8006/#v1:0:18:4.....53>

PROXMOX Virtual Environment 8.2.2

Vista por servidor

Centro de datos

- vm-proxmox-c02
 - Qinq100 (vm-proxmox-c02)
 - Qinq200 (vm-proxmox-c02)
 - localnetwork (vm-proxmox-c02)
 - NFS-Compartido-ISO (vm-proxmox-c02)
 - local (vm-proxmox-c02)
 - local-lvm (vm-proxmox-c02)
 - Pool_ASIR1_alum1
 - Pool_ASIR1_alum2
 - Pool_PROF_profe1
 - Pool_PROF_profe2
 - Pool_TIC_alum3
 - Pool_TIC_alum4

Centro de datos

- Roles
- Dominios
- HA
- SDN**
- Zonas
- VNets
- Opciones
- IPAM
- ACME
- Cortafuego

Estado

SDN	Nodo	Estado
localnet...	vm-proxmox-c02	ok
Qinq100	vm-proxmox-c02	available
Qinq200	vm-proxmox-c02	available

Imagen de elaboración propia: Creación de las dos Qinq en el nodo 2 de Proxmox al igual que hemos hecho en el nodo 1 (CC BY-NC-SA)

Crea 4 contenedores en el nodo 1 de Proxmox, asignándoles IP según la siguiente tabla:



CLIENTE CPD	ID CONTENEDOR	IP CONTENEDOR	Zona QinQ	VNet VLAN
1	1001	10.0.1.110/16	QinqZona100	SQ100-10
	1002	10.0.1.130/16		SQ100-30
2	2001	10.0.1.210/16	QinqZona200	SQ200-10
	2002	10.0.1.230/16		SQ200-30

Ahora, crea 4 contenedores en el nodo 2 de Proxmox, asignándoles IP según la siguiente tabla:

CLIENTE CPD	ID CONTENEDOR	IP CONTENEDOR	Zona QinQ	VNet VLAN
1	1021	10.0.2.110/16	QinqZona100	SQ100-10
	1022	10.0.2.130/16		SQ100-30
2	2021	10.0.2.210/16	QinqZona200	SQ200-10
	2022	10.0.2.230/16		SQ200-30

De tal manera que el CT1001 solo puede hacer ping al CT1021 y viceversa, y no podrá hacer ping al resto de contenedores porque se encuentra el tráfico de tramas Ethernet aislado por su QinQ:

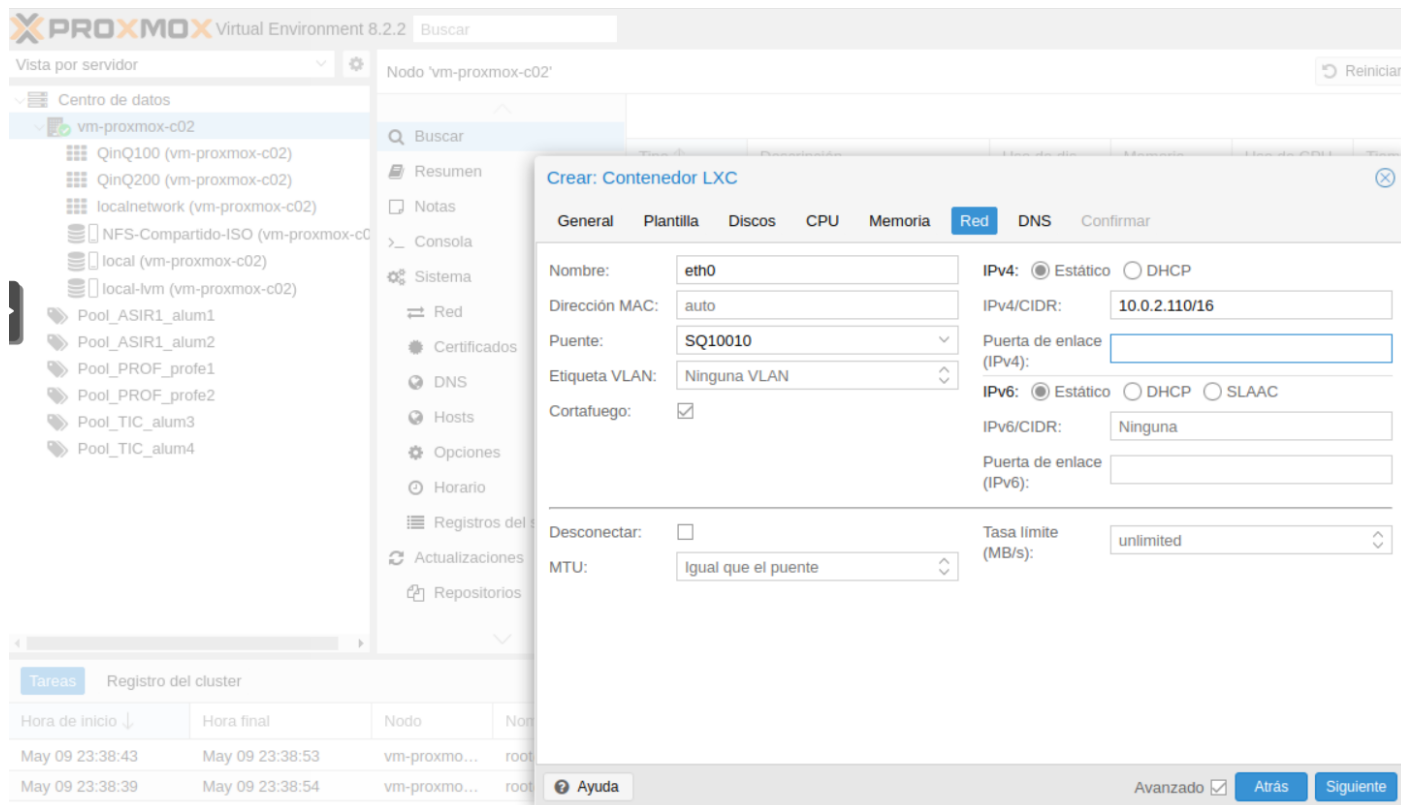


Imagen de elaboración propia: Creación del contenedor 1021 (CC BY-NC-SA)

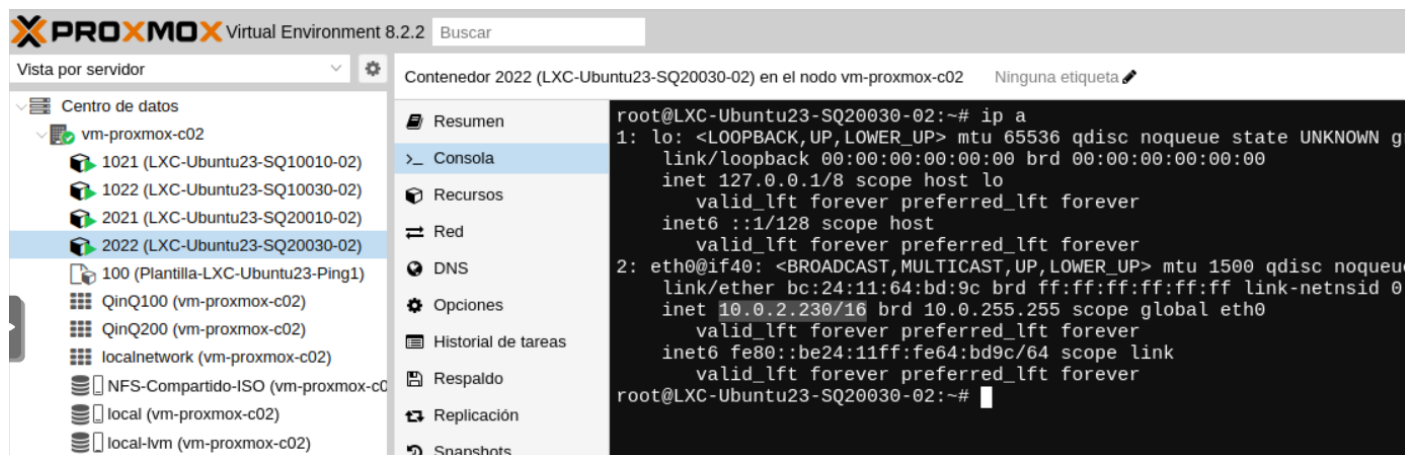


Imagen de elaboración propia: Configuración de red del contenedor 2022 (CC BY-NC-SA)



The screenshot shows the Proxmox Virtual Environment 8.2.2 interface. On the left, the 'Centro de datos' sidebar lists the VM '1001 (LXC-Ubuntu23-SQ10010-01)'. The main console window displays the terminal output for this VM. The user has logged in as root and executed a series of commands: 'run-parts: /etc/update-motd.d/98-fsck-at-reboot exited with return code 2', 'Last login: Thu May 9 11:08:54 UTC 2024 on lxc/tty1', and a 'ping 10.0.2.110'. The output shows successful ping results: 'PING 10.0.2.110 (10.0.2.110) 56(84) bytes of data. 64 bytes from 10.0.2.110: icmp_seq=1 ttl=64 time=7.01 ms', '64 bytes from 10.0.2.110: icmp_seq=2 ttl=64 time=1.19 ms', and '64 bytes from 10.0.2.110: icmp_seq=3 ttl=64 time=1.03 ms'. The user then enters '^C' to stop the ping.

Imagen de elaboración propia: Ping desde el CT 1010 del nodo 1 al CT 2010 del nodo 2 y rechazados todos los demás (CC BY-NC-SA)

The screenshot shows the Proxmox Virtual Environment 8.2.2 interface. On the left, the 'Centro de datos' sidebar lists the VM '1001 (LXC-Ubuntu23-SQ10010-01)'. The main console window displays the terminal output for this VM. The user has executed a series of 'ping' commands to various IP addresses: 'ping 10.0.2.130', 'ping 10.0.2.210', and 'ping 10.0.2.230'. The output shows that all these ping attempts failed with 'Destination Host Unreachable' and '100% packet loss'. The user then enters '^C' to stop the ping.

Imagen de elaboración propia: Rechazados todos los ping al resto de CT tal y cómo se esperaba (CC BY-NC-SA)

Revisión #1

Creado 11 mayo 2024 20:09:23 por Daniel Cano Verdú

Actualizado 12 mayo 2024 16:53:02 por Daniel Cano Verdú