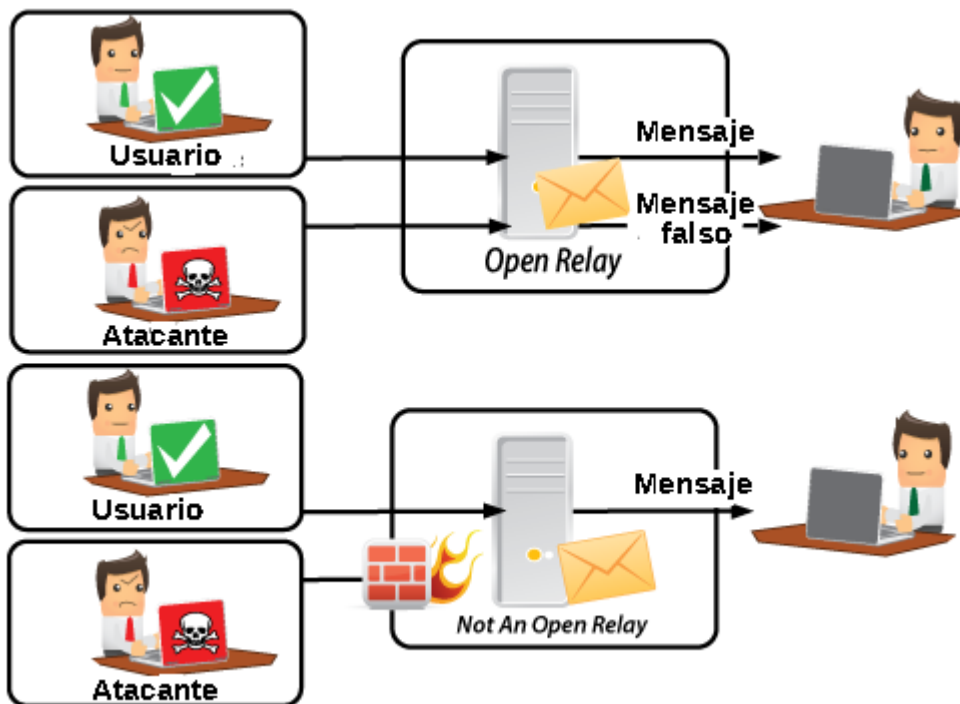


Configurar envíos no autorizados de correos (Open Relay)

Se entiende como "open relay" un servidor SMTP configurado de tal manera que permite que cualquier usuario de Internet lo use para enviar correo electrónico a través de él.



1. Servidor de correo no configurado de manera segura

1.1. Comprobar si nuestro servidor es un "open relay"

Podemos comprobar si nuestro servidor es un "open relay" (a correos internos) con la siguiente herramienta: <http://www.dnsexit.com/Direct.sv?cmd=testMailServer>

From email address:

To email address:
(must be the domain's address)

Email server name:

SMTP Port:

Check Email Server

```
Connecting correo. .gob.bo:25
resp <-      220 ESMTP IMSVA
send ->      helo correo. .gob.bo
resp <-      250 imsva .gob.bo
send ->      mail from:<sistemas@.gob.bo>
resp <-      250 2.1.0 Ok
send ->      rcpt to:<info@.gob.bo>
resp <-      250 2.1.5 Ok
send ->      data
resp <-      354 End data with <CR><LF>.<CR><LF>
send ->      Subject: DNS Exit Email Test
send ->      Please ignore this email.
Test email by MX testing tool at
http://www.dnsExit.com/Direct.sv?cmd=testMailServer
send ->
resp <-      250 2.0.0 Ok: queued as 0BCD7D6046
```

Servidor vulnerable

Successful !! correo. .gob.bo is OK to receive emails for .gob.bo

Podemos comprobar si nuestro servidor es un "open relay" (a correos externos): <https://mxtoolbox.com/SuperTool.aspx>

https://mxtoolbox.com/SuperTool.aspx?action=mx

MX TOOLBOX®

Home MX Lookup Blacklists Diagnostics Domain Health Analyze

SuperTool Beta7

mail[redacted].gob.bo Test Email Server

smtp:mail[redacted].gob.bo Monitor This Solve Email Delivery Problems

Are you confident that your email is getting delivered?
You rely on email for business critical communication, so you need to know your email need to know who is sending email on your behalf.

220 mail[redacted].gob.bo ESMTP Postfix

1.2. Deshabilitando Open Relay (Postfix 3.x en Debian 9)

En el archivo `/etc/mail/main.cf`

Declaran los dominios a los que se autorizará mandar mensajes a través de nuestro servidor:

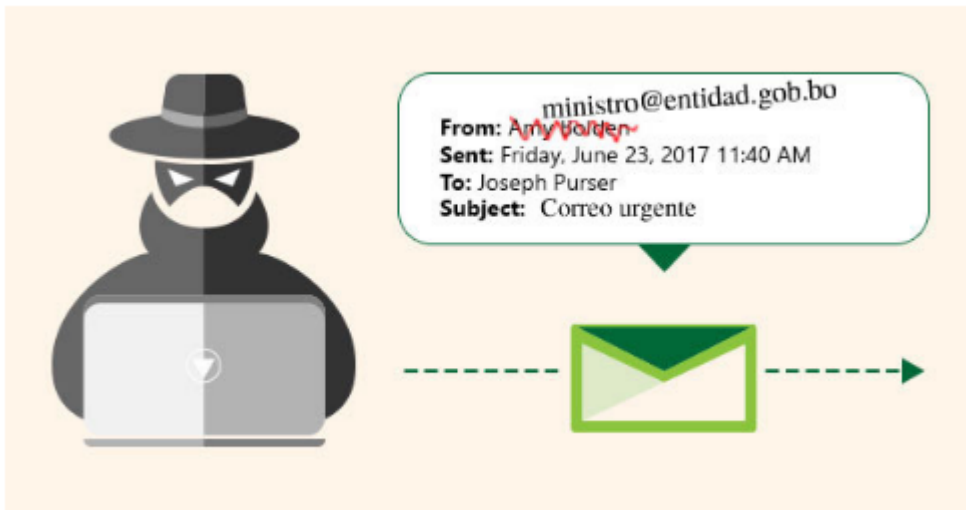
```
relay_domains = mientidad.com
```

Configurar la lista de direcciones IPs que pueden mandar correos. (Típicamente solo la IP del servidor de correos):

```
mynetworks = 192.168.40.2/32
```

2. Servidor DNS no configurado de manera segura

Un atacante puede falsificar el remitente de los correos modificando los header:



2.1. Configurar el registro PTR

En una zona de mapeo inverso, un registro PTR mapea una dirección IP a un nombre de host.

Editar el archivo de configuración de zona directa (Por ejemplo: db.empresa.com) y agregar:

correo	IN	A	200.129.81.150
empresa.com.	IN	MX	10 correo.empresa.com

“correo” es el nombre de subdominio para el servidor de correo de “empresa.com” y “200.129.81.150” la IP del servidor de correo y 10 es el número de preferencia del servidor de correo.

Tenga en cuenta que pueden existir múltiples hosts de servidores de correo, ambos deberían estar incluidos por ejemplo:

correo1	IN	A	200.129.81.150
correo2	IN	A	200.129.81.151
empresa.com.	IN	MX	10 correo1.empresa.com.
empresa.com.	IN	MX	10 correo2.empresa.com.

Editar el archivo de configuración de zona inversa (Por ejemplo: db.81.129.200) y agregar:

150	IN	PTR	correo.empresa.com.
-----	----	-----	---------------------

Para el caso de múltiples hosts de servidores de correo:

150	IN	PTR	correo1.empresa.com.
151	IN	PTR	correo2.empresa.com.

Verificamos la configuración de la siguiente manera:

```
$ dig empresa.com MX

;; ANSWER SECTION:
empresa.com.          3600    IN      MX      10      correo.empresa.com.

$ host correo.empresa.com

correo.empresa.com has address 200.129.81.150

$ dig @1.1.1.1 -x 200.129.81.150

;; ANSWER SECTION:
150.81.129.200.in-addr.arpa. 18282 IN      PTR      correo.empresa.com.
```

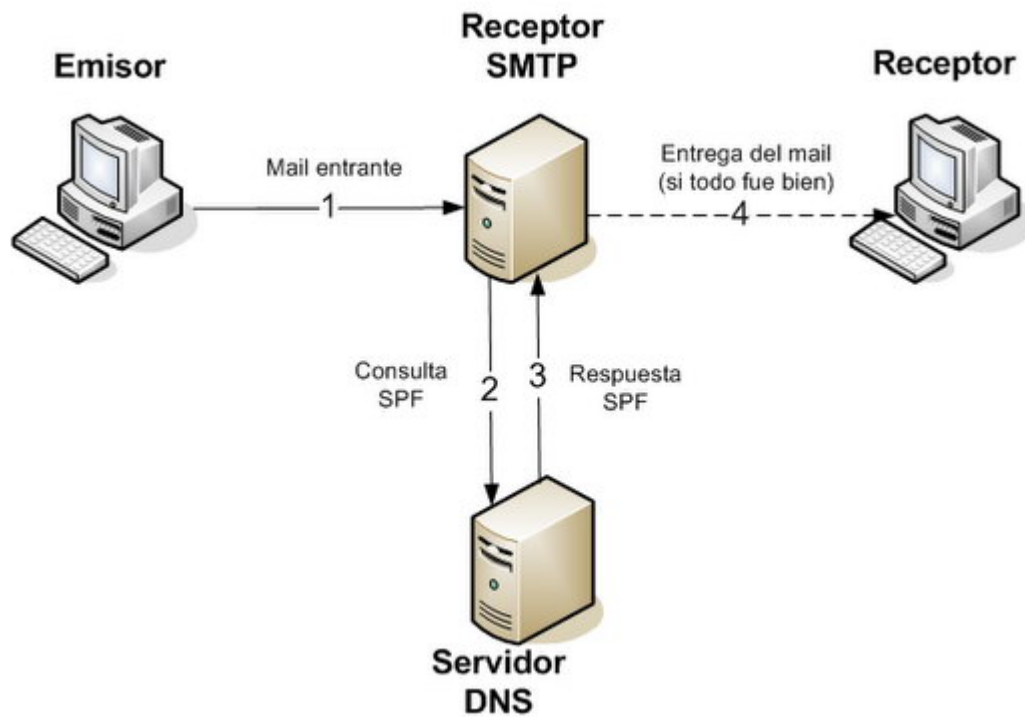
NOTA. La resolución de la zona inversa PTR del host del servidor de correo debe corresponder a la especificada en el registro SPF

2.2. Registro SPF

Sender policy Framework (SPF), registro que ayuda a prevenir el envío de correos electrónicos no autorizados desde tú dominio (conocido como spoofing), en consecuencia, si tú dominio no tiene configurado este registro es posible que servidores que tienen implementado esta política rechacen o marquen el correo como spam.

El servidor que recibe el correo electrónico compara el dominio del mismo con la lista de los equipos autorizados para realizar el envío de mensajes desde ese dominio. Según el registro, el servidor decide si dejar que el correo se envíe y se entregue al destinatario o, por el contrario bloquearlo.

2.2.1. ¿Cómo funciona?



Comprobar si tenemos configurado SPF en nuestro dominio:

<https://mxtoolbox.com/SuperTool.aspx>

MX TOOLBOX® Upgrade

Home MX Lookup Blacklists Diagnostics Domain Health Analyze Headers Free Mo

SuperTool Beta7

miempresa.com

SPF Record Lookup

spf:miempresa.com Find Problems Solve Email Delivery Problems Vulnerable

	Test	Result
✖	DNS Record Published	DNS Record not found

2.2.2. ¿Cómo configurar el registro TXT?

Usar la siguiente herramienta:

<https://mxtoolbox.com/SPFRecordGenerator.aspx?domain=entidad.gob.bo&prefill=true>

Deberá llenar desde que dominios e IPs envía correos electrónicos:

SPF WIZARD

Answer the questions below and we'll generate a record for you in the correct format. If you have questions, you can contact [MxToolbox Support](#)

Do you send email from your webserver?

Yes ▼

Do you send email from the same server in your MX records?

Yes ▼

Enter any other server hostname or domain that delivers email for your domain

correo.empresa.com

Enter your domain's IP Addresses / CIDR Ranges

190.129.78.150

Enter any 3rd party systems that may deliver emails for your domain (usually provided to you by the sending system)

Ex. Google Apps, Office 365, etc., This record is usually provided by the 3rd party.

How strict should the SPF Policy be?

Strict ▼

El registro generado con la herramienta deberá ser configurado en el servidor de DNS:

Create Domain

Domain Name	Updated
 :domain.com	May 22, 2012

Record Type: TXT Record

Host Name: :domain.com

Text:

Time to Live (TTL) Minutes

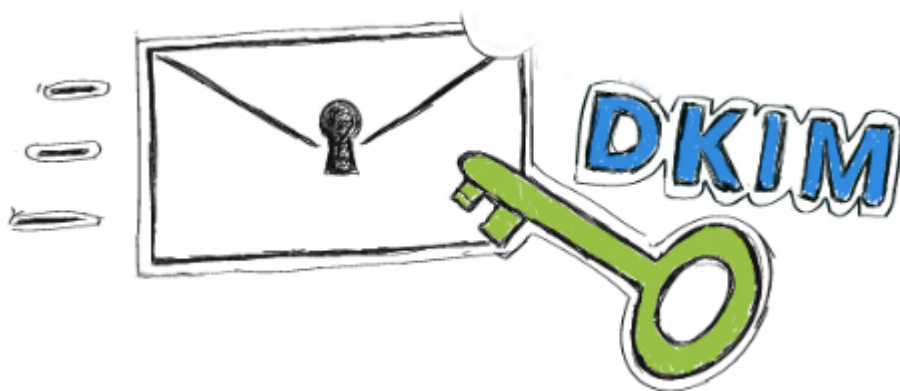
Add Record [Cancel](#)

Una vez configurado el servidor DNS tardara un tiempo en propagarse.

2.2.3. ¿Cómo funciona el registro TXT?

El servidor de correo destinatario verificará el correo entrante con los registros TXT del dominio origen, si se llega a comprobar correctamente dejará pasar el correo añadiendo la cabecera Received-SPF

2.3. Registro DKIM



2.3.1. ¿Qué es DKIM?

Es un mecanismo de autenticación de correo electrónico (estándar que proviene del inglés Domain Keys Identified Mail) que ayuda a prevenir el spoofing en los mensajes enviados desde nuestro dominio.

2.3.2. ¿Cómo funciona?

DKIM implementa una clave pública con la que firma la cabecera de cada correo saliente. Al llegar al servidor receptor, éste descifra el encabezado mediante DKIM y verifica que el contenido del correo se íntegro (sin modificaciones).

2.3.3. ¿Cómo configurar DKIM?

Primero se debe generar un par de claves y con esto también se generará el registro TXT para el servidor DNS, que tendrá un aspecto parecido a:

```
dkim._domainkey.empresa.com IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC65tv6LhAbbrqcgwgyBaC
x50scjedj357we9SJdff6VH0KDYgU/kvuV2rQiedHjtJDPuFJIwoNqh8pbIWxcZ8J2FhVhXU1QWdBm0Q/w61jfsyVAMrX/Src
JAd/1 XHYcS4o3uIOV7jICV0JLiYW5wjYlvWpPoraQzQE1NpjlSx2T5QIDAQAB" ; ----- DKIM key default for
midominio.gob.bo
```

Ahora se debe editar el archivo de configuración del DNS y agregar el registro TXT que se genere de acuerdo a nuestro dominio.

La configuración varía de acuerdo a cada servidor de correo

El DNS queda parecido a:

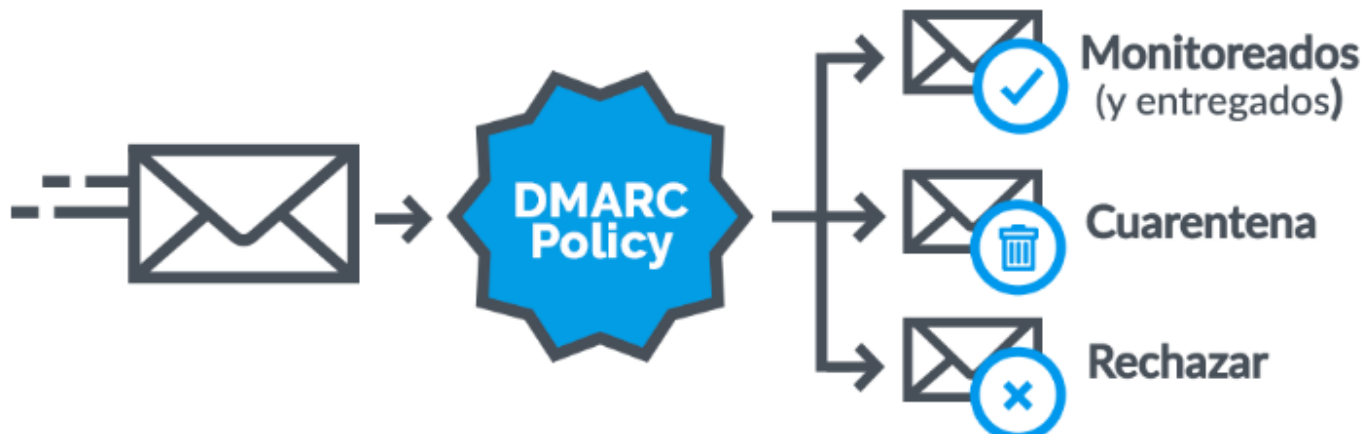
```
root@[REDACTED]:/etc/bind# cat db.empresa.com
; ZONA EXTERNA DIRECTA
; /etc/bind/db.empresa.com
; empresa.com
$TTL 604800
@ IN SOA DNS.empresa.com. root.DNS.empresa.com. (
    3 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
; name server NS records
@ IN NS dns.empresa.com.
@ IN A 107.0.22.35
; name server A records
dns IN A 107.0.22.35
; A records
mail IN A 107.0.22.35
; MX records
@ IN MX 10 mail.empresa.com.
dkim._domainkey.empresa.com. TXT v=DKIM1;p=MIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEAtFVCgVvvMfR2Ir05kvayXbXbvxd6dE
YeLe9XthDLjWI2mhaHWYbiNsyhQwjuRskJLQ1x30RJqUx0Ezu1YQevW4ruojbSN04KCHpaN27zFpT6bLS0PXZbt0P5q21Et1Ees3x3xHPEVmHuxhQar0FJJ1V/iwc
KePIVnVAzTk9feYnM74LyL5EdHGZjmnDa18EGPcPYe9GZwjpZf4iTh9xFFmHu2FG73s47oRebQ0l8NXC38sLs8My9n1BuDiJnJ9ow/svDcyKquuxC4mQYHsTM0Cv
7XvRabJJYTs1A3EMew9JH7TjyE/hzT0NcB60Myox7ND5r1FXvhpuQxi0xZwMPQIDAQAB 300
```

Listo, ahora todos los correos enviados serán seguros y tendrán un aspecto parecido a este:

```
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@zimbra.io header.s=C172B774-D1DA-11E7-99E2-34CB6CB9DD9A header.b=Odna2KiC;
spf=pass (google.com: domain of jdelacruz@zimbra.io designates 178.62.48.7 as permitted sender) smtp.mailfrom=jdelacruz@zimbra.io;
dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=zimbra.io
Return-Path: <jdelacruz@zimbra.io>
Received: from mail.zimbra.io (mail.zimbra.io. [178.62.48.7])
by mx.google.com with ESMTPS id p14si454331wr.35.2017.11.25.04.27.23
for <jorgedlcruz@gmail.com>
(version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
Sat, 25 Nov 2017 04:27:23 -0800 (PST)
Received-SPF: pass (google.com: domain of jdelacruz@zimbra.io designates 178.62.48.7 as permitted sender) client-ip=178.62.48.7;
Authentication-Results: mx.google.com;
dkim=pass header.i=@zimbra.io header.s=C172B774-D1DA-11E7-99E2-34CB6CB9DD9A header.b=Odna2KiC;
spf=pass (google.com: domain of jdelacruz@zimbra.io designates 178.62.48.7 as permitted sender) smtp.mailfrom=jdelacruz@zimbra.io;
dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=zimbra.io
Received: from localhost (localhost [127.0.0.1]) by mail.zimbra.io (Postfix) with ESMTP id C329A1616C5 for <jorgedlcruz@gmail.com>; Sat, 25 Nov 2017 12:27:22 +0000 (GMT)
Received: from mail.zimbra.io ([127.0.0.1]) by localhost (mail.zimbra.io [127.0.0.1]) (amavisd-new, port 10032) with ESMTP id OtKfPWT_m13o for <jorgedlcruz@gmail.com>; Sat, 25 Nov 2017 12:27:22 +0000 (GMT)
Received: from localhost (localhost [127.0.0.1]) by mail.zimbra.io (Postfix) with ESMTP id 71AD816179A for <jorgedlcruz@gmail.com>; Sat, 25 Nov 2017 12:27:22 +0000 (GMT)
DKIM-Filter: OpenDKIM Filter v2.10.3 mail.zimbra.io 71AD816179A
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=zimbra.io; s=C172B774-D1DA-11E7-99E2-34CB6CB9DD9A; t=1511612842; bh=0H22raPE2vVJ7gebQbP9PFSaLcd22qBrvf519Ipeb5xk=;
h=Date:From:To:Message-ID:MIME-Version; b=Odna2KiCA7a/HnOdApPafQGsBrqVQaMM6DKvSfE7BSglB047JcG+Dmt/UpjuH+naV
1Cj43uUSwCVKHoRtBuz/4tdF2GzSRhWQp5sjv4llicxk+N6vtRiYvOMV6qID77C
6VoB5bFARaL7bEkrftkw7kGi0WuOzUPzbytykfDwzd5cFP4hUCVHz1CqNvd7d8u
NF2k7iZ/RN03AKQ26/1auqs7Kyt/yJQl0ccKrEP6viSAuve8gPWHZ/5zk0X6I0oEDQ
F1mGFJbaVXztVORAonbk9XQ8EXOR2kvlbQj4F8HSU+EvP59voWRBh21xwyp12VcW9v
BTuZgFhuazFQoa
X-Virus-Scanned: amavisd-new at zimbra.io
Received: from mail.zimbra.io ([127.0.0.1]) by localhost (mail.zimbra.io [127.0.0.1]) (amavisd-new, port 10026) with ESMTP id I6SeKrHHT_i for <jorgedlcruz@gmail.com>; Sat, 25 Nov 2017 12:27:22 +0000 (GMT)
Received: from mail.zimbra.io (mail.zimbra.io [178.62.48.7]) by mail.zimbra.io (Postfix) with ESMTP id 49A9B1616C5 for <jorgedlcruz@gmail.com>; Sat, 25 Nov 2017 12:27:22 +0000 (GMT)
Date: Sat, 25 Nov 2017 12:27:22 +0000 (GMT)
From: Jorge de la Cruz <jdelacruz@zimbra.io>
To: jorgedlcruz <jorgedlcruz@gmail.com>
Message-ID: <1802838606.190.1511612842250.JavaMail.zimbra@zimbra.io>
Subject: Hello
MIME-Version: 1.0
```

2.4. Registro DMARC

DMARC indica cómo debe manejarse los correos que fallen las comprobaciones SPF y DKIM. Existen 3 opciones de para tratar un correo que falle la comprobación SPF y DKIM:



Podemos usar la herramienta en línea <https://mxtoolbox.com/SuperTool.aspx> para comprobar el registro DMARC.

MX TOOLBOX® Upgrade

Home MX Lookup Blacklists Diagnostics Domain Health Analyze Headers Free M

SuperTool Beta7

miempresa.com

DMARC Lookup

dmARC:miempresa.com Find Problems Solve Email Delivery Problems

	Test	Result
x	DNS Record Published	DNS Record not found

2.4.1. Adicionando registro DMARC en el servidor DNS

Adicionar un registro TXT en el servidor DNS con el siguiente contenido:

```
v=DMARC1; p=quarantine;  
rua=mailto:dmARC@miempresa.com  
ruf=mailto:dmARC@miempresa.com; sp=quarantine
```

Revision #4

Created 1 marzo 2023 16:10:57 by Vladimir Urquiola

Updated 10 abril 2024 11:05:56 by Franz Rojas