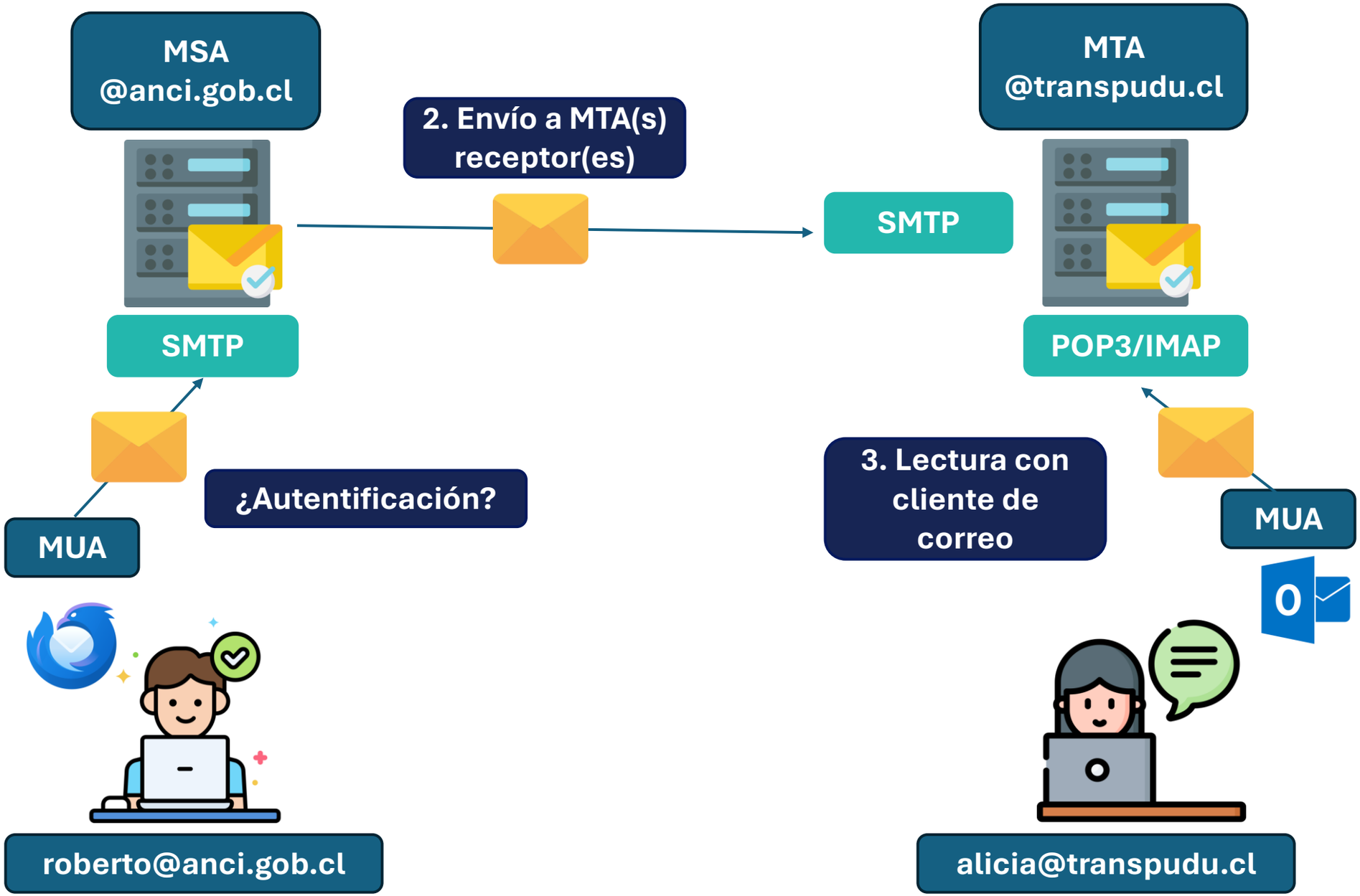
ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

Correo Electrónico seguro: Uso eficaz de SPF/DKIM/DMARC

Eduardo Riveros Roca
Profesional
Agencia Nacional de Ciberseguridad

¿Cómo funciona el correo electrónico?

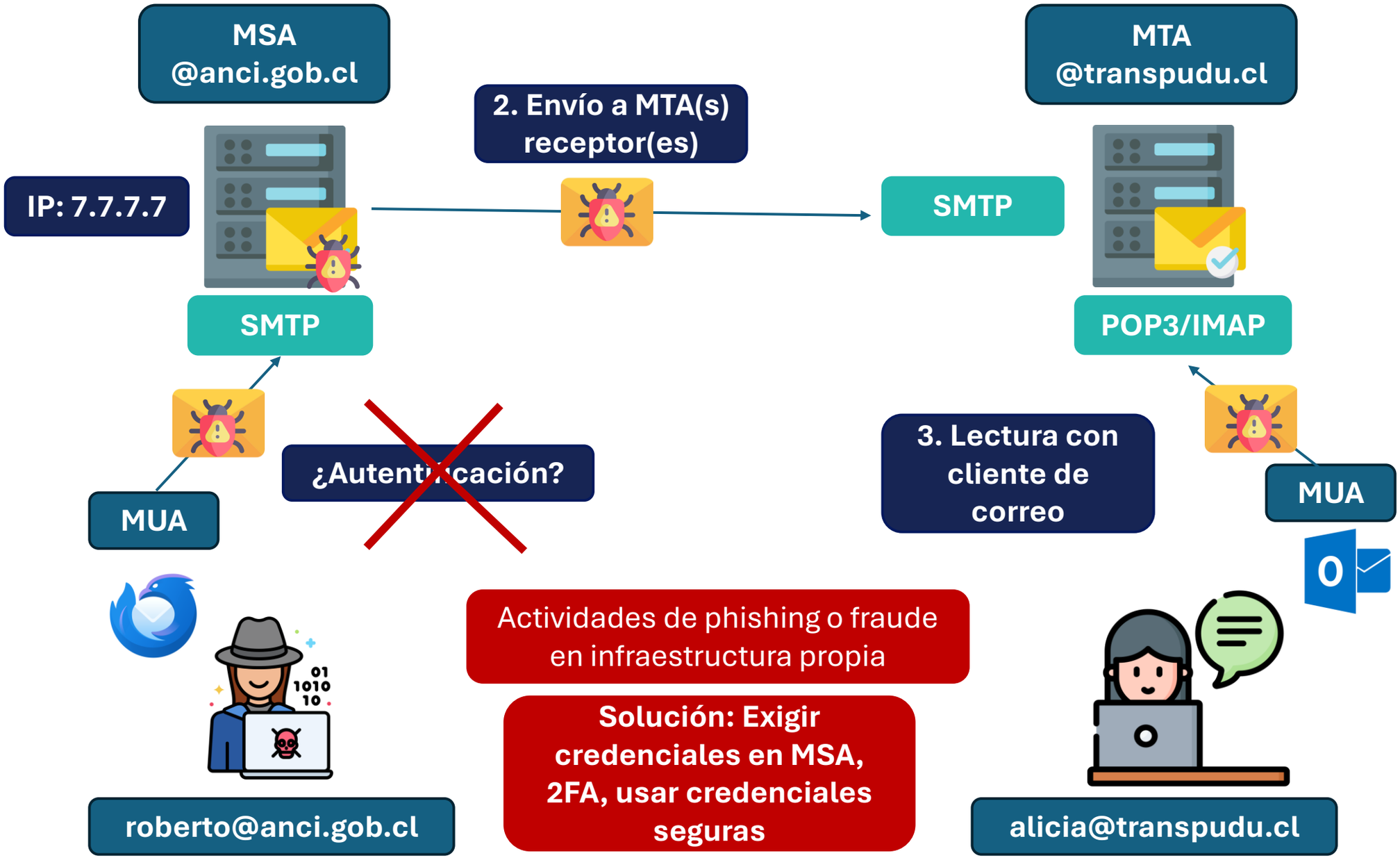
¿Cómo funciona el correo electrónico?



Potenciales ataques

Uso no autorizado de servidores de correo

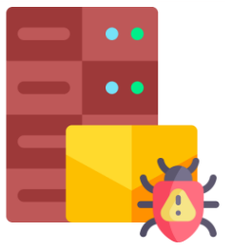
ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD



Suplantación

MSA no oficial (configurado para @anci.gob.cl)

IP: 6.6.6.6



SMTP

MUA

roberto@anci.gob.cl

2. Envío a MTA(s) receptor(es)

Actividades de phishing o fraude relacionadas con la institución

Solución: En esta charla

MTA @transpudu.cl

SMTP

POP3/IMAP

3. Lectura con cliente de correo

MUA

alicia@transpudu.cl

Compromiso de Integridad

MSA
@anci.gob.cl

IP: 7.7.7.7

SMTP

MUA

2. Envío a MTA(s) receptor(es)

MTA comprometido
@transpudu.cl

SMTP

POP3/IMAP

MUA

3. Lectura con cliente de correo

roberto@anci.gob.cl

alicia@transpudu.cl

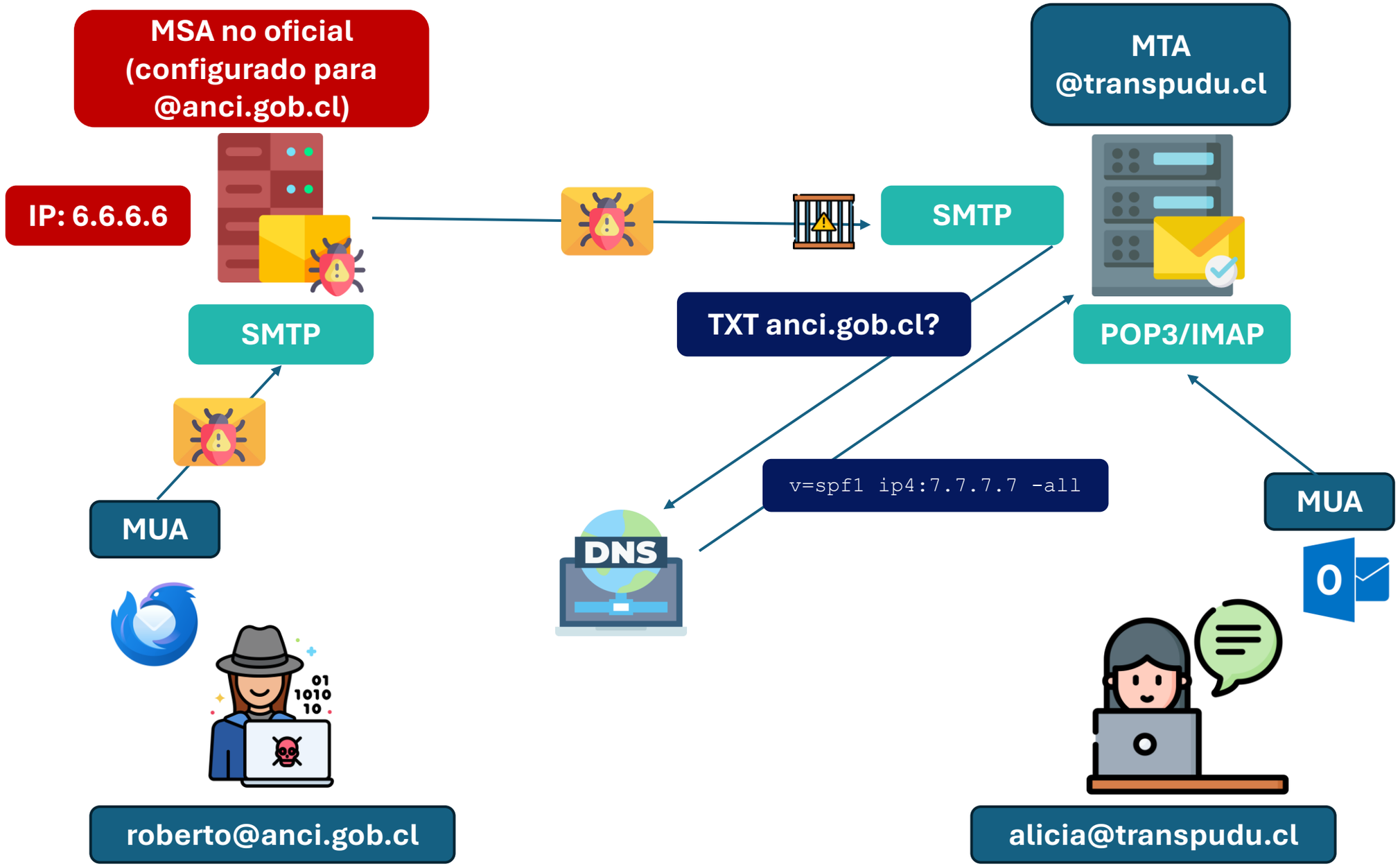
Actividades de phishing o fraude en infraestructura propia

Solución: En esta charla

SPF+DKIM+DMARC como mitigación

SPF, o quién puede y quien no puede enviar correos a mi nombre

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD



Ejemplos SPF

https://www.rfc-editor.org/rfc/rfc7208

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

`v=spf1 +all`

Cualquier IP pasa el chequeo.

`v=spf1 mx:anci.gob.cl -all`

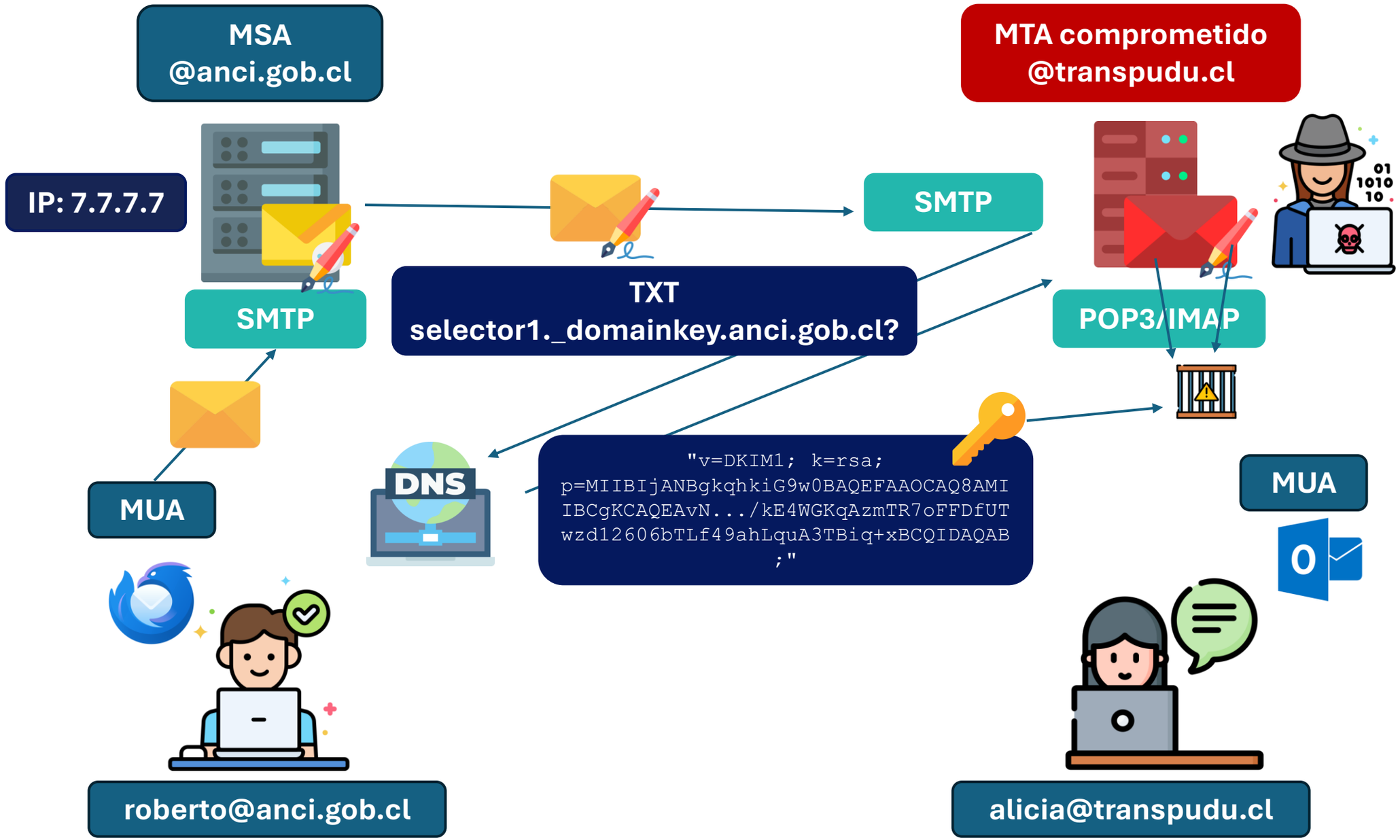
Pasan solo las IPs asociadas por un registro **MX** a **anci.gob.cl**

`v=spf1 ip4:192.0.2.128/28 -all`

Pasan solo las IPs en la subred **192.0.2.128/28**

Recomendación: Usar siempre *–all* al final, definir solo IPs/dominios que envían correos

DKIM, o firmas criptográficas para asegurar integridad



Estructura de mensaje con DKIM

```
X-Authentication-Results: transpudu.cl
     header.from=roberto@anci.gob.cl; dkim=pass
Received: from mout23.football.example.com (192.168.1.1)
     by shopping.example.net with SMTP;
```

Agregado por MDU

```
DKIM-Signature: v=1; a=rsa-sha256; s=selector1; d=anci.gob.cl;
        c=simple/simple; q=dns/txt; i=joe@football.example.com;
        h=Received : From : To : Subject : Date : Message-ID;
        bh=2jUSOH9NhtVGCQWNr9BrIAPreKQjO6Sn7XIkfJVOzv8=;
        b=AuUoFEfDxTDkHlLXSZEpZj79LICEps6eda7W3deTVFOk4yAUoqOB
        4nujc7YopdG5dWLSdNg6xNAZpOPr+kHxt1IrE+NahM6L/LbvaHut
        KVdkLLkpVaVVQPzeRDI009SO2Il5Lu7rDNH6mZckBdrIx0orEtZV
        4bmp/YzhwvcubU4=;
Received: from client1.anci.gob.cl  [192.0.2.1A]
        by submitserver.anci.gob.cl with SUBMISSION;
        Fri, 25 Jul 2025 10:31:54 -0400
```

Agregado por MSA

```
From: Roberto Cripto <roberto@anci.gob.cl>
To: Alicia Grafía <alicia@transpudu.cl>
Subject: ¿Vamos a almorzar?
Date: Fri, 25 Jul 2025 10:30:37 -0400
Message-ID: <20030712040037.46341.5F8J@anci.gob.cl>

Hola.

¿Almorcemos juntos hoy? Podemos ir al Subway a comprar algo.

Roberto.
```

Mensaje original

- https://www.rfc-editor.org/rfc/rfc6376.html

DKIM, o firmas criptográficas para asegurar integridad

1. Crear par de llaves criptográficas

2. Configurar llave privada en MSA

Agregar RR DKIM en DNS de dominio de correo

Recomendación: Usar llave RSA de 2048 bits o superior. Usar suplementariamente algoritmos de firma modernos (como ed25519)

DMARC, o qué hago si detecto algo raro en un correo que recibo de tu dominio

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

```
v=DMARC1; p=POLICY;
rua=MAILTO:DMARC_REP
ORT_EMAIL;
ruf=MAILTO:DMARC_REP
ORT_EMAIL
```

v	Versión DMARC
p	Política
rua	Dirección de correo electrónico para los informes de DMARC.
ruf	Dirección de correo electrónico para los informes DMARC fallidos

None	El correo electrónico que no pasa la autenticación DMARC se entregará.
Quarantine	El correo electrónico que no pasa la autenticación DMARC se entregará.
Reject	El correo electrónico que no pasa la autenticación DMARC se rechazará.

Usar reject como política

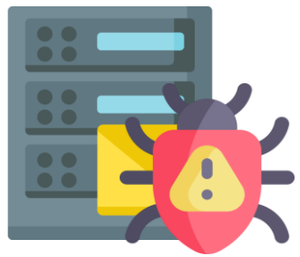
Revisar reportes o integrarlos a una herramienta que permita visualizarlos

https://domainaware.github.io/parsedmarc/

https://www.rfc-editor.org/rfc/rfc7489

¿SPF+DKIM+DMARC son infalibles?

Phishing con dominios similares



Vulnerabilidades en MSA/MTA/MUA

Exfiltración de llaves privadas (DKIM)

Pérdida de control de IP/dominio configurado en SPF

Servidores de recepción en incumplimiento

Referencias y agradecimientos

- Guía SPF/DKIM/DMARC CSIRT de Gobierno (2024): https://csirt.gob.cl/documents/4563/Manual_SPF_DKIM_y_DMARC.pdf
- RFC 7208 (SPF): https://www.rfc-editor.org/rfc/rfc7208
- RFC 6376 (DKIM): https://www.rfc-editor.org/rfc/rfc6376.html
- RFC 7489 (DMARC): https://www.rfc-editor.org/rfc/rfc7489
- ParseDMARC (Herramienta OSS): https://domainaware.github.io/parsedmarc/
- Íconos e ilustraiones obtenidas desde FlatIcon: https://flaticon.com

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

Correo Electrónico seguro: Uso eficaz de SPF/DKIM/DMARC

¿Dudas?
ayuda@anci.gob.cl