Una experiencia en el uso de DMARC

Santiago Aggio

CCTBB – UTN FRBB

LACNIC 24 / LACNOG 2015
Bogotá, Colombia

DMARC

Domain-based Message Authentication, Reporting, and Conformance (RFC 7489, March 2015)

- **Autenticación:** Alineación del resultado de dos mecanismos conocidos: SPF y DKIM
- **Reporte:** Recibo y Generación de reportes periódicos
- **Conformidad:** aplica una política a partir del resultado de la alineación.

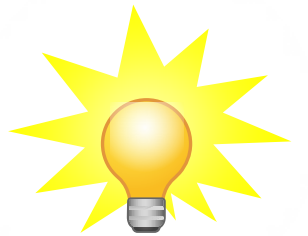
Sender Policy Framework (SPF)

- Identifica que servidores están autorizados a enviar correo para un dominio
- Permite verificar que un mensaje es originado desde un host o IP autorizados para el dominio del remitente de dicho mensaje
- RFC 4408 (RFC 7208, RFC 6652)
- Simple Registro TXT en DNS
- Dominio que autoriza envíos solo desde sus MX:

dominio IN TXT “v=spf1 mx -all”

- Dominio que no envía emails:

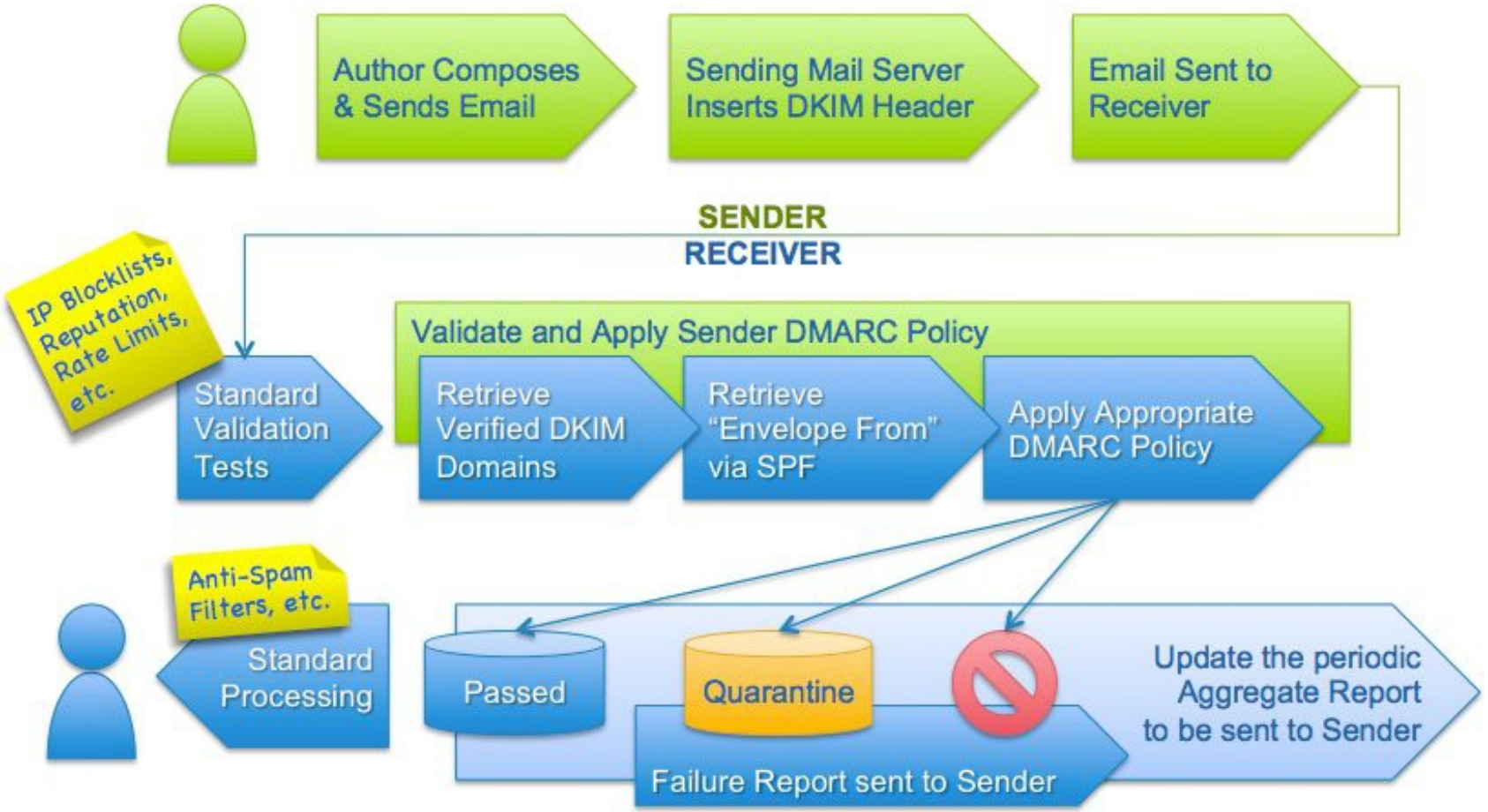
dominio IN TXT “v=spf1 -all”



DKIM

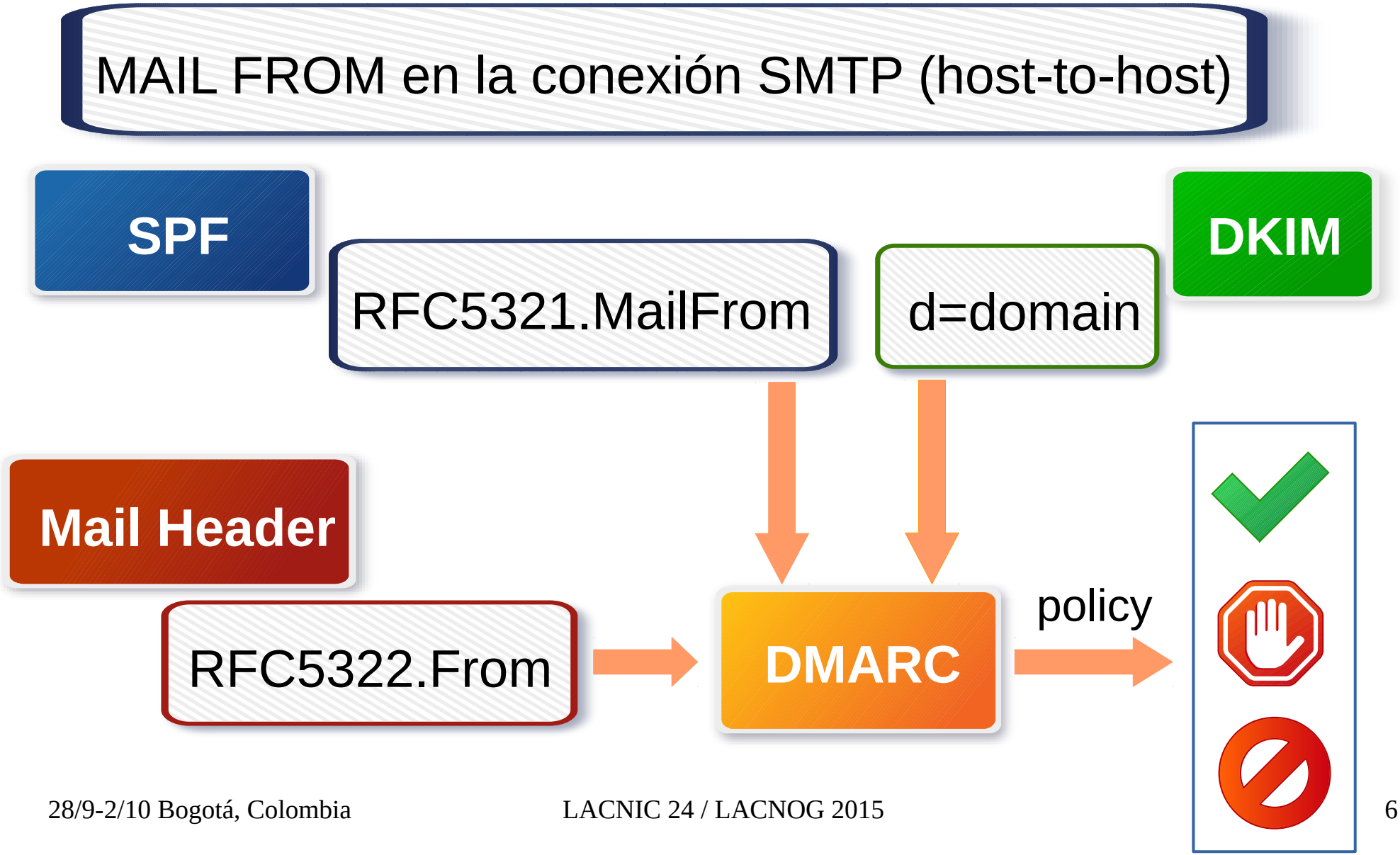
- Domain Keys Identified Mail (2004, Yahoo)
- Firma digital con cifrado de clave Pública y Privada
- Firma con clave privada los mensajes salientes de un dominio
- El receptor verifica con la clave pública obtenida del DNS:
  - El dominio del remitente
  - Partes seleccionadas del mensaje no fueron modificadas después del envío
- Resuelve el problema de falsificación del remitente
- No resuelve el problema del SPAM y Phishing

DMARC: Proceso de Autenticación



https://dmarc.org/overview/

Alineación de Identificadores



DMARC: registro DNS

v	Protocol version	v=DMARC1
pct	Percentage of messages subjected to filtering	pct=20
ruf	Reporting URI for forensic reports	ruf=mailto:authfail@example.com
rua	Reporting URI of aggregate reports	rua=mailto:aggrep@example.com
p	Policy for organizational domain	p=quarantine
sp	Policy for subdomains of the OD	sp=reject
adkim	Alignment mode for DKIM	adkim=s
aspf	Alignment mode for SPF	aspf=r

DMARC: Políticas en MP's

- Yahoo (Abril de 2014)

```
$ dig +short txt _dmarc.yahoo.com

"v=DMARC1\; p=reject\; sp=none\; pct=100\; rua=mailto:dmarc-
yahoo-rua@yahoo-inc.com, mailto:dmarc_y_rua@yahoo.com\;"
```

- Gmail

```
dig +short txt _dmarc.gmail.com

"v=DMARC1\; p=none\; rua=mailto:mailauth-reports@google.com"
```

- Twitter (Febrero de 2013)

```
dig +short txt _dmarc.twitter.com

"v=DMARC1\; p=reject\; rua=mailto:d@rua.agari.com\;
ruf=mailto:d@ruf.agari.com\; fo=1"
```

DMARC: Políticas en MP's

- Facebook

```
$ dig +short txt _dmarc.facebook.com

"v=DMARC1\;
p=reject\;pct=100\;rua=mailto:d@rua.agari.com,mailto:postmaster@facebook
.com\; ruf=mailto:d@ruf.agari.com\;"
```

- Linkedin

```
$ dig +short txt _dmarc.linkedin.com

"v=DMARC1\; p=reject\;
rua=mailto:d@rua.agari.com,mailto:dmarc_agg@auth.returnpath.net\;
ruf=mailto:d@ruf.agari.com,mailto:dmarc_afrf@auth.returnpath.net\;
pct=100"
```

- Paypal

```
dig +short txt _dmarc.paypal.com

"v=DMARC1\; p=reject\; rua=mailto:d@rua.agari.com\;
ruf=mailto:dk@bounce.paypal.com,mailto:d@ruf.agari.com"
```

DMARC Reportes

- De Agregación (Global)
  - Se agregan los resultados de la autenticación en un único reporte.
  - Formato XML
  - Dirección IP fuente, resultados de la autenticación y disposición de la política.
  - Se envían a diario

- De Fallo
  - Se generan en casos especiales y cuando la autenticación falla (DoS)
  - Específico de un mensaje y se incluye el encabezado
  - Formato ARF (RFC 5965) / AFRF (RFC 6591)

DMARC Reporte de Agregación

```
<record>
    <row>
      <source_ip>192.168.2.2</source_ip>
      <count>2</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>fail</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
    <identifiers>
      <header_from>example.com</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>example.com</domain>
        <result>fail</result>
        <human_result></human_result>
      </dkim>
      <spf>
        <domain>example.com</domain>
        <result>pass</result>
      </spf>
    </auth_results>
  </record>
```

DMARC: Problemas

- Envíos con SMTP autenticado desde direcciones de dominios ajenos o externos
  - Permitir solo el envío desde dominios propios y autorizados
- Registros con dirección externa al dominio
  - Foros y Portales educativos (Ej: Moodle)
  - Envíos por intermediarios (Ej: BlackBerry)
- Clientes SMTP
  - Monitoreo con reportes por mail (host no autorizado)
    - Nagios, fail2ban, etc
- MX Secundarios no autorizados

DMARC: Listas de correo

- Problemas
  - Notorio a partir del cambio de política de algunos MP's
  - Mensajes rechazados por falla en la verificación
  - Usuarios pueden ser dados de baja de la lista
  - Puede bajar la reputación del sitio que contiene la lista (alta tasa de rechazos)
  - Usuarios de dominios DMARC p=”reject” no son permitidos
  - Remapeo a usuarios locales para simular reply y posterior forward
  - Criterio y política final por parte del administrador de la lista.
- Mailman
  - Soluciones y parches en http://wiki.list.org/DEV/DMARC

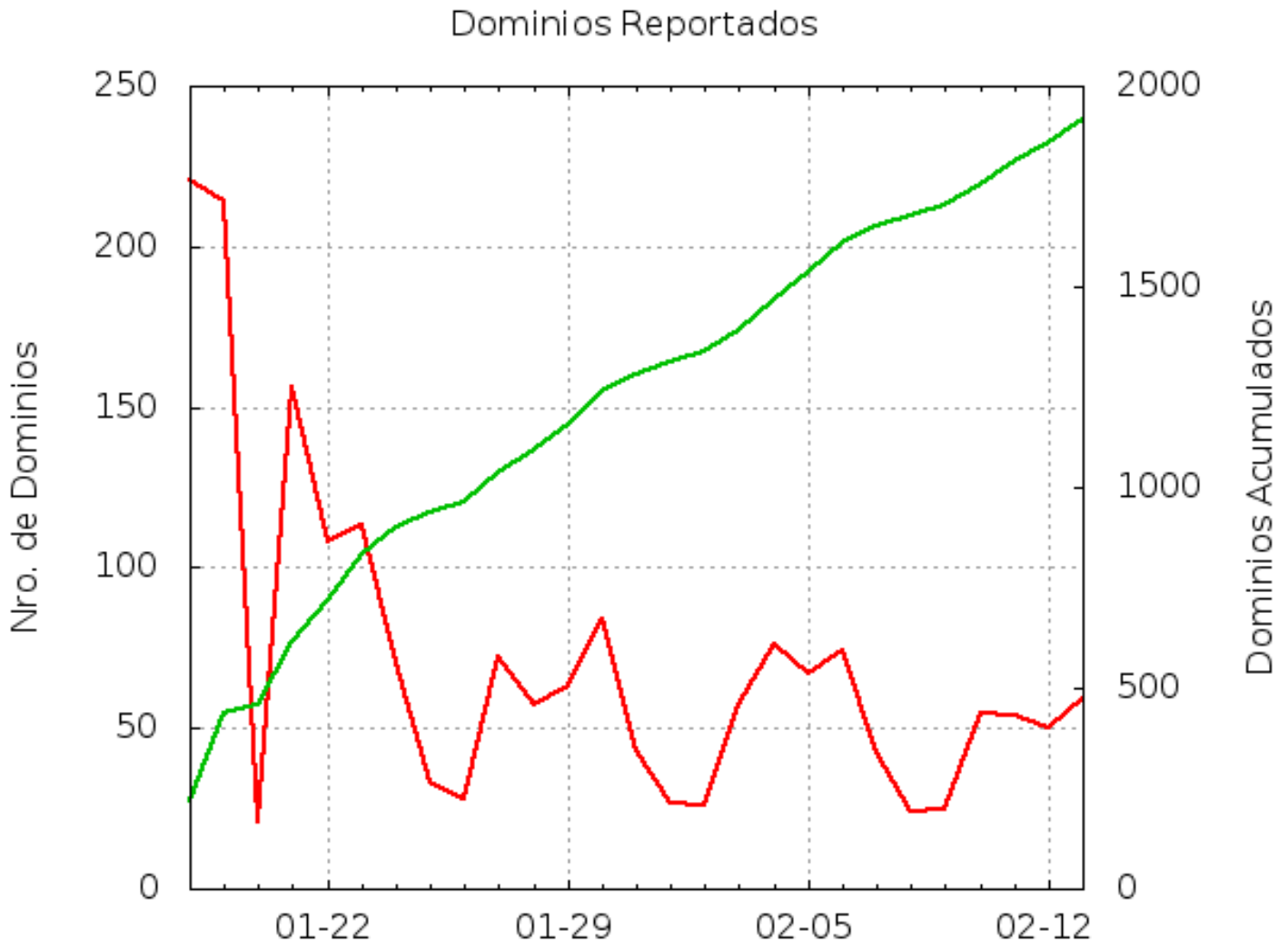
Implementación DMARC

- SPF implementado con anterioridad.
- **Mayo de 2014:** Implementación de DKIM con opendkim
- **Junio de 2014:** Registro _dmarc TXT en DNS
  - policy=none
  - Primer reporte de microsoft.com 3 Jun 2014 13:16:50 -0700
- **Enero de 2015:** Implementación de DMARC con opendmarc para envío de reportes
- **Agosto de 2015:** Reportes generados (6 meses)

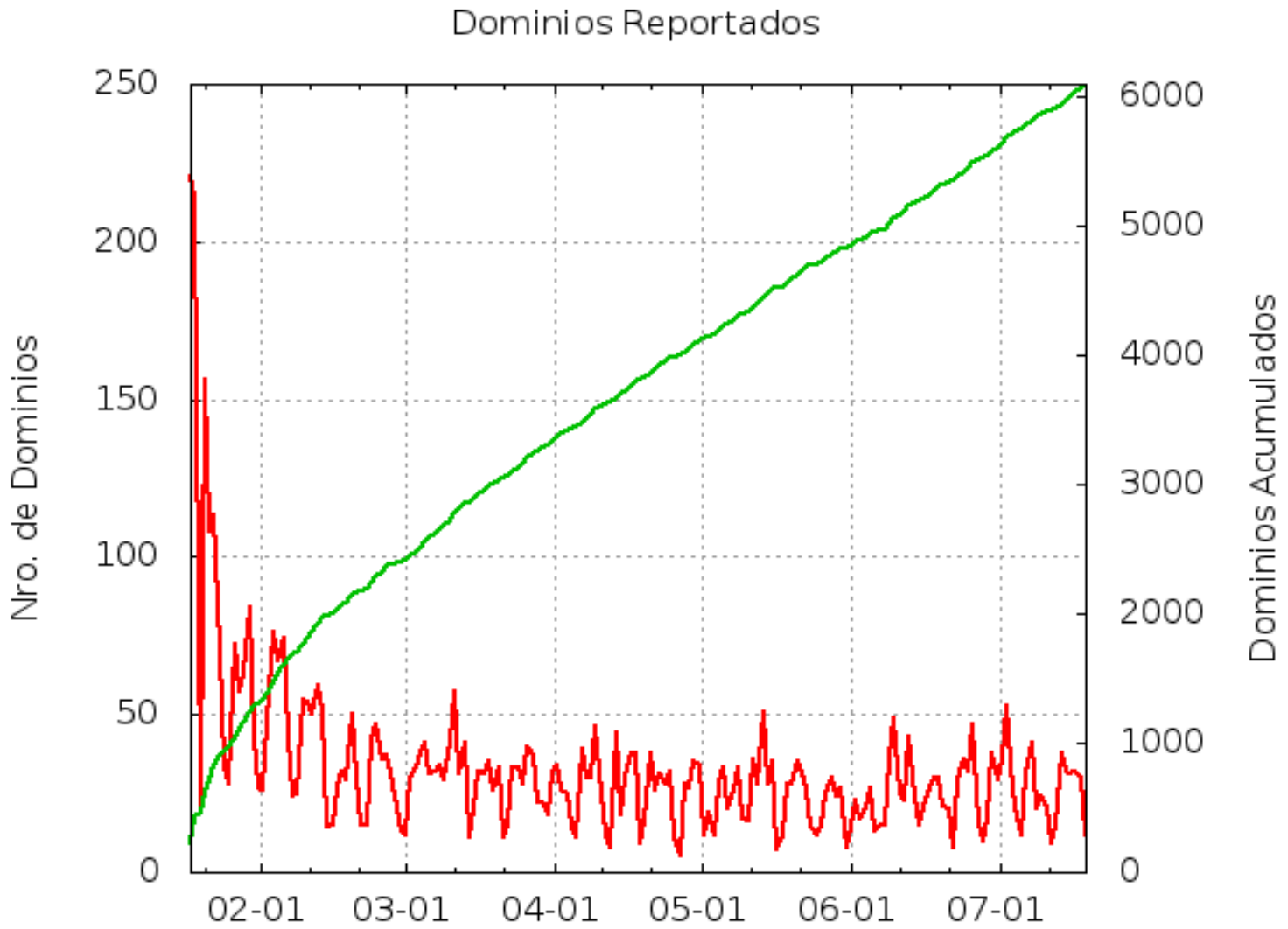
Reportes Recibidos (Jun14-Jul15)

Organización	Rep	Men	F && F	F || F	P && P	otros	IPv4	IPv6
google.com	421	213232	1.5	12.3	**69.3**	16.9	26.3	**73.7**
Microsoft Corp.	407	284136	0.0	13.7	**30.0**	**56.2**	100.0	0.0
Yahoo! Inc.	372	68981	0.0	1.3	**80.5**	18.2	100.0	0.0
facebook.com	196	455	0.0	0.0	22.0	**78.0**	100.0	0.0
intertek.com	98	98	0.0	0.0	0.0	**100.0**	100.0	0.0
linkedin.com	67	178	0.0	0.0	6.7	**93.3**	55.6	44.4
Comcast.net	60	326	0.0	0.6	**91.4**	8.0	7.4	**92.6**
cisco.com	59	61	0.0	0.0	8.2	**91.8**	18.0	**82.0**
ipb.pt	33	35	0.0	0.0	0.0	**100.0**	0.0	**100.0**
dhl.com	18	19	0.0	0.0	10.5	**89.5**	100.0	0.0
ox.com	13	13	0.0	0.0	0.0	**100.0**	100.0	0.0
geosoft.com	10	10	0.0	0.0	0.0	**100.0**	100.0	0.0
<10 Reportes	34	61	0.0	4.9	23.0	72.1	80.3	19.7
25	1788	567605	0.01	11.65	50.92	36.84	72.22	27.78

Reportes Generados (25 días)



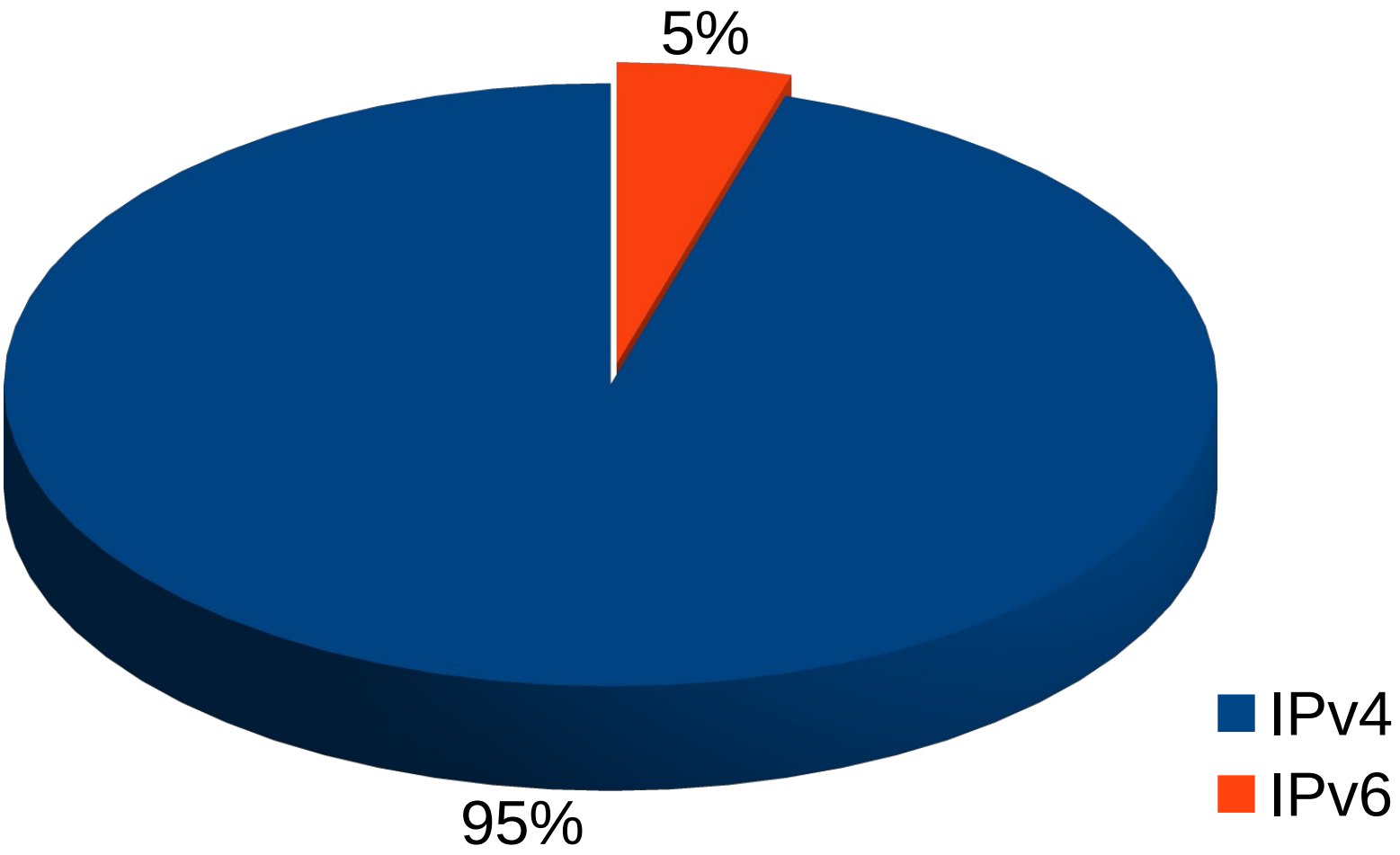
Reportes Generados (6 meses)



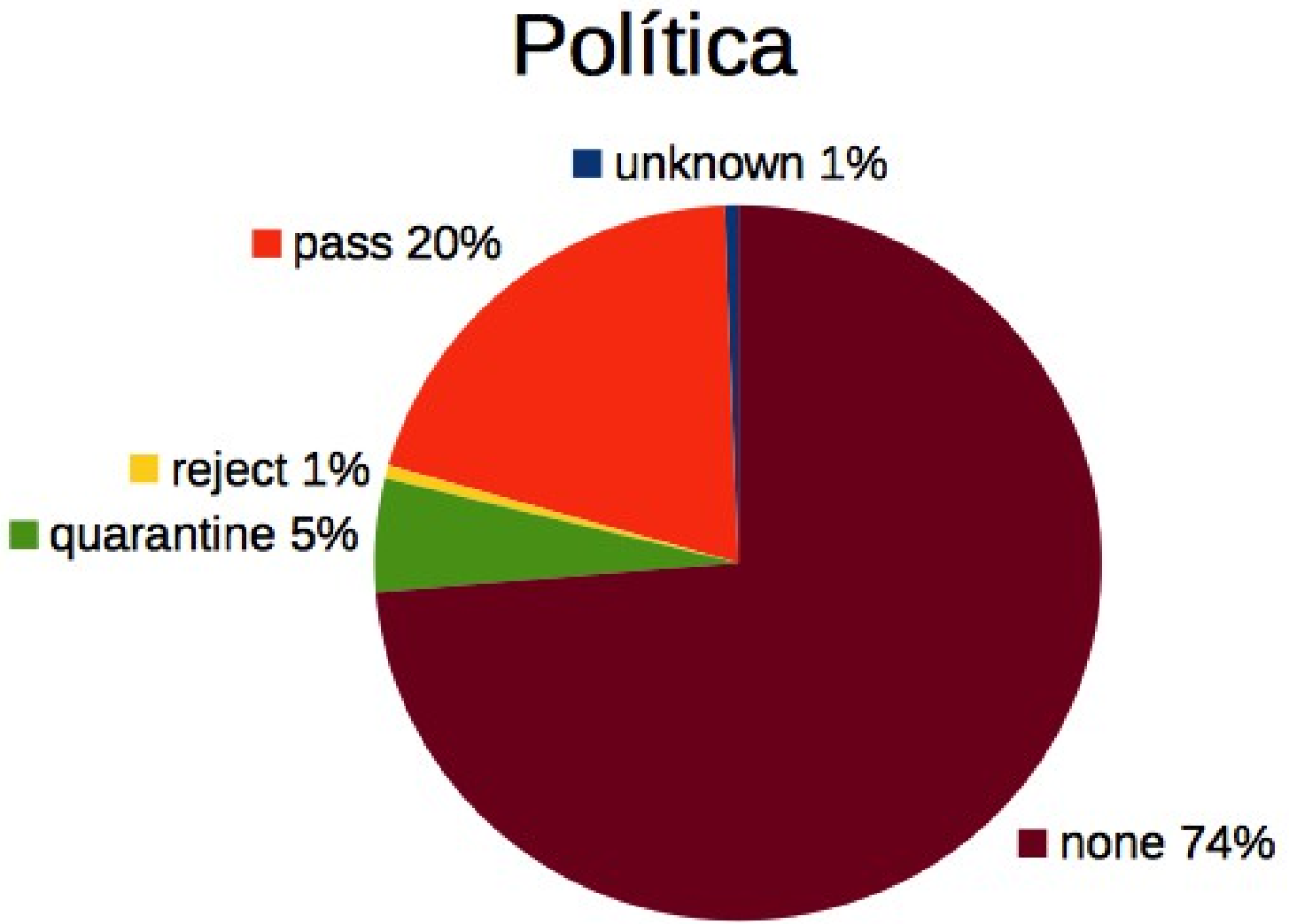
Reportes Generados

Dominio	IP	%
NXDOMAIN	3354	11.06
yahoo.com	2771	9.14
speedy.com.ar	1891	6.24
google.com	865	2.85
hotmail.com	680	2.24
amazonses.com	636	2.10
yahoo.co.jp	419	1.38
rr.com	387	1.28
xmailix.net	373	1.23
linkedin.com	364	1.20
t-ipconnect.de	355	1.17
mcsv.net	348	1.15
movistar.net.ar	324	1.07
Otros	17106	57.89

Reportes Generados



DMARC: Análisis de Reportes

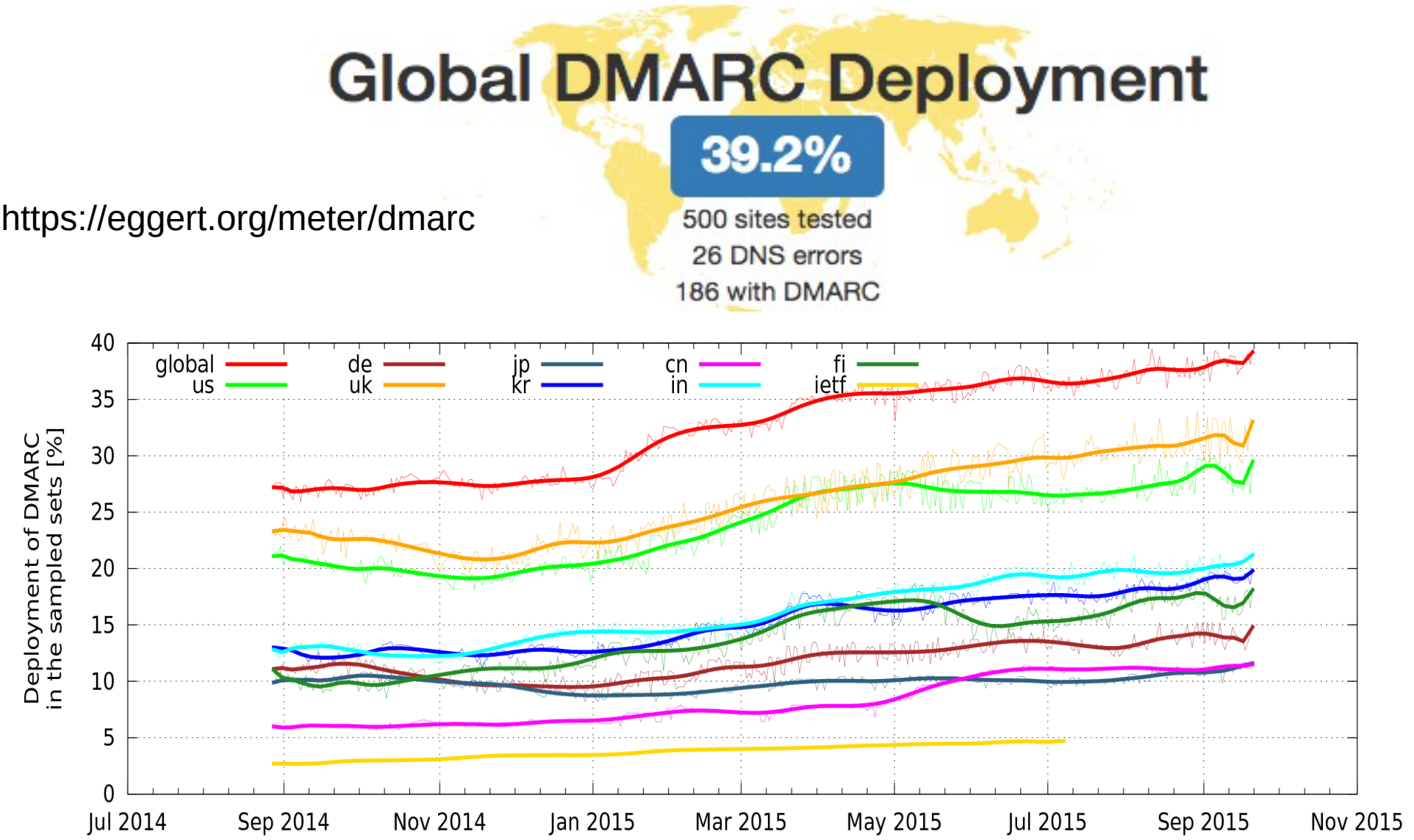


Pasos de Implementación

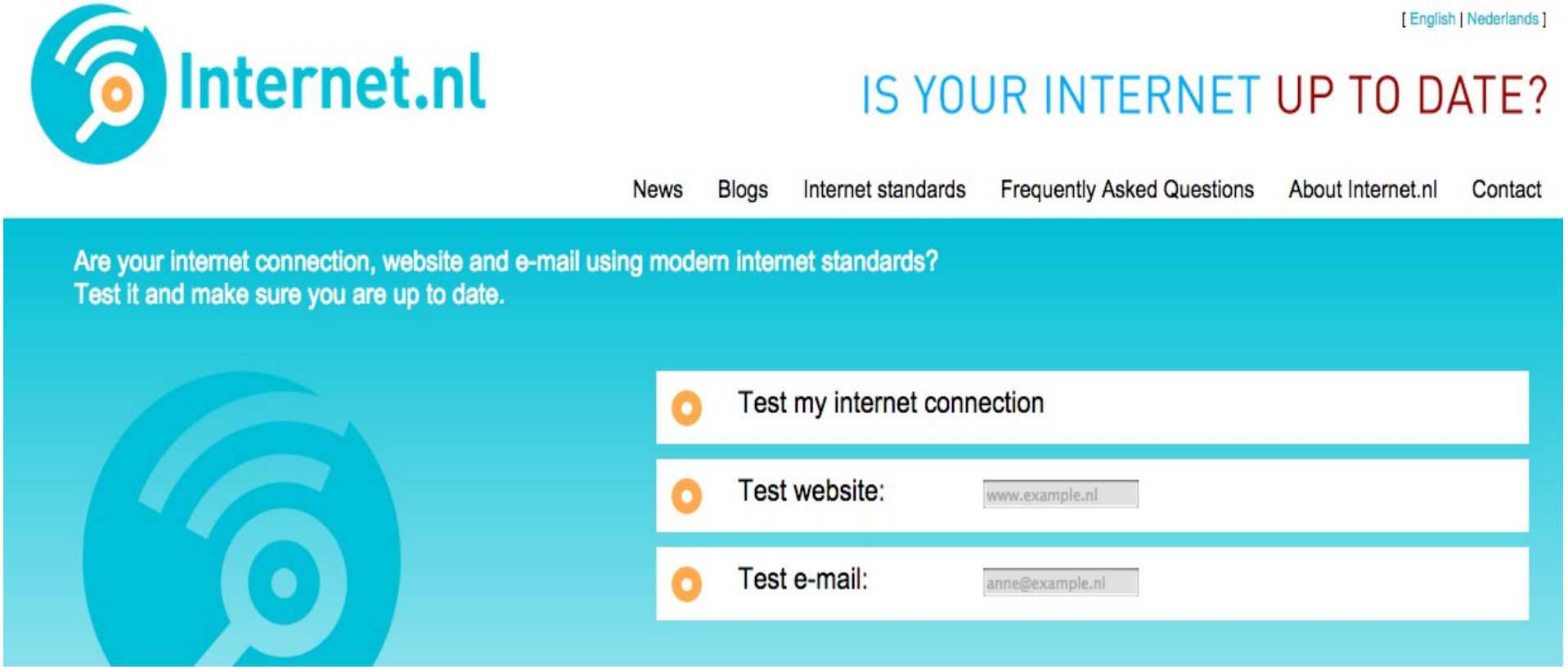
- Definir registro TXT para SPF en el DNS (-all)
- Implementar DKIM
  - Registro DNS y firma de mensajes
- Definir Registro _dmarc.dominio en el DNS (p=none)
  - Recibir reportes
- Implementar DMARC
  - Verificar alineación y generar reportes
- Cambiar política cuando estemos seguros
  - p=quarantine o.... **p=reject**

DMARC: Despliegue Global

https://eggert.org/meter/dmarc



Test IPv6, DNSEC, TLS, DKIM/SPF/DMARC



http://www.internetsociety.org/deploy360/blog/2015/04/internet-nl-provides-an-easy-way-to-test-your-ipv6-dnssec-and-tls/

Conclusión

- Baja implementación.
- Mejorar las herramientas de análisis de reportes
- Pocas implementaciones de código abierto
- Más uso de DNS
- Adoptado por los grandes proveedores de email
- Los reportes ayudan a corregir errores en el uso
- Identifica y combate el fraude del remitente

¿Es DMARC la solución?

FIN

¿Preguntas?

slaggio@criba.edu.ar