GLOBAL CYBER ALLIANCE

DMARC Bootcamp

Shehzad Mirza

Director de operaciones

smirza@globalcyberalliance.org

gca-dmarc@globalcyberalliance.org

¿Qué es DMARC?

Las reglas DMARC permiten a los remitentes indicar que sus mensajes están protegidos y les dicen a los destinatarios qué deben hacer con los mensajes que fallen la validación (por ejemplo, enviarlos a Spam o rechazarlos directamente).

¿Qué se necesita para implementar DMARC?

- Conocer los sistemas o servidores de correo de la organización
- Acceso a nivel administrador al DNS de la organización
- Lista de subdominios, si los hubiera
- SPF y DKIM (si ya estuvieran instalados)

Registro de texto en el DNS para DMARC

- Configuración básica:

  Host: _dmarc

  Valor: v=DMARC1; p=none; rua=mailto:*<dirección de correo>*; ruf=mailto:*<dirección de correo>;*

- Configuración compleja:

  Host: _dmarc

  Valor: v=DMARC1; p=none; rua=mailto:*<dirección de correo>*; ruf=mailto:*<dirección de correo>*; fo=1; adkim=r; aspf=r; pct=100; rf=afrf; ri=86400; sp=reject;

¿Qué significa cada etiqueta?

Obligatorias:

- v=DMARC1 → versión
- p= → política (regla) aplicable
- rua= → informes agregados

Recomendadas:

- ruf= → informes forenses / de rechazos

Tal vez necesaria:

- **sp=** → política para subdominios

Opcionales:

- **fo=** → envía muestras de mensajes que no han pasado los controles SPF o DKIM
- **adkim=** → modo de alineación DKIM
- **aspf=** → modo de alineación SPF
- **pct=** → % de mensajes afectados
- **rf=** → formato de informes
- **ri=** → intervalo entre informes

Las etiquetas DMARC en detalle (I)
p=

Define la regla (o política) de DMARC que debe aplicarse:

“v=DMARC1; p=none;” → sin acción

“v=DMARC1; p=quarantine;” → cuarentena

“v=DMARC1; p=reject;” → rechazar

DMARC

¿Qué les ocurre a los mensajes?

- Depende de la regla que se haya configurado:
  - **None (sin acción):** se alerta de posibles mensajes sospechosos, pero todos acaban llegando al buzón de entrada
  - **Quarantine (cuarentena):** los mensajes que no pasen los controles de SPF y DKIM ni de alineación son enviados a la carpeta de correo basura
  - **Reject (rechazar):** los mensajes que no pasen los controles de SPF y DKIM ni de alineación son rechazados y nunca llegan a entregarse
- Se aconseja empezar en *None* e ir pasando poco a poco a *Reject*

Las etiquetas DMARC en detalle (II)
rua= y ruf=

rua= → informes agregados

ruf= → informes forenses (de rechazos)

"v=DMARC1; p=none; rua=mailto:<*dirección de correo*>; ruf=mailto:<*dirección de correo*>;"

Ejemplos:

"v=DMARC1; p=none; rua=mailto:**dmarc-rua**@empresa.com; ruf=mailto:**dmarc-ruf**@empresa.com;"

"v=DMARC1; p=none; rua=mailto:**dmarc-rua**@empresa.com, mailto:admin@empresa.com; ruf=mailto:**dmarc-ruf**@company.com;"

Las etiquetas DMARC en detalle (III)
fo=

Opcional: se utiliza para los informes forenses o de rechazos

• envía muestras de mensajes que no han pasado los controles SPF o DKIM

"v=DMARC1; p=none; rua=mailto:<*dirección de correo*>; ruf=mailto:<*dirección de correo*>; fo=<0,1d,s>"

0 → valor predeterminado: se generará un informe cada vez que todos los mecanismos de autenticación fallen

1 → se generará un informe cada vez que alguno de los mecanismos de autenticación den algún resultado diferente de una validación con alineación

d → se generará un informe de fallo de validación DKIM por cada mensaje que contenga alguna firma que no haya pasado la autenticación, con independencia de la alineación

s → se generará un informe de fallo SPF por cada mensaje que no pase la validación SPF, con independencia de la alineación

Las etiquetas DMARC en detalle (IV) adkim= y aspf=

Opcionales: definen el modo de alineación para DKIM y SPF, respectivamente

"v=DMARC1; p=none; rua=mailto:<*dirección de correo*>; ruf=mailto:<*dirección de correo*>; fo=1; adkim=<s,r>; aspf=<s,r>"

s → alineación estricta

r → alineación laxa **(valor predeterminado)**

Las etiquetas DMARC en detalle (V)
rf= y ri=

Opcionales

"v=DMARC1; p=none; rua=mailto:<*dirección de correo*>; ruf=mailto:<*dirección de correo*>; fo=1; adkim=r; aspf=r; rf=<afrf>; ri=<*segundos*>"

rf= → formato de informes

- **afrf (valor predeterminado)** → formato ARF (Abuse Report Format*, RFC 5965)
- **iodef** → formato IODEF (Incident Object Description Exchange Format*, RFC 5070)

ri= → intervalo entre informes, en segundos

- El valor predeterminado es 84600 (24 horas)

*En español: formato de notificación de vulneraciones (ARF) y formato para el intercambio de descripciones de objetos de incidentes (IODEF)

Las etiquetas DMARC en detalle (VI)
pct=

Opcional

"v=DMARC1; p=none; rua=mailto:<*dirección de correo*>; ruf=mailto:<*dirección de correo*>; fo=1; adkim=r; aspf=r; rf=afrf; ri=84600; pct=<0-100>"

- Valor: 0-100 (el valor predeterminado es 100)
- Usar 'p=quarantine; pct=0;' equivale a usar p=none
- Usar 'p=reject; pct=0;' equivale a usar p=quarantine

Las etiquetas DMARC en detalle (y VII)
sp=

Opcional, pero conviene plantearse si es realmente necesario utilizarla

"v=DMARC1; p=none; rua=mailto:<*dirección de correo*>; ruf=mailto:<*dirección de correo*>; fo=1; adkim=r; aspf=r; rf=afrf; ri=86400; sp=<*regla DMARC*>;"

- Aplica las mismas reglas que p=, pero a todos los subdominios
  - Si no se define, el valor predeterminado será el de p=
- Cuándo debe utilizarse:
  - Cuando no haya subdominios y aún se esté en p=none, se recomienda usar sp=reject
  - Cuando haya varios subdominios y la organización esté lista para dar el paso a p=reject o p=quarantine, se recomienda usar sp=none

Registro de texto en el DNS para DMARC

- Configuración básica:

  Host: _dmarc

  Valor: v=DMARC1; p=none; rua=mailto:*<dirección de correo>*; ruf=mailto:*<dirección de correo>;*

- Configuración compleja:

  Host: _dmarc

  Valor: v=DMARC1; p=none; rua=mailto:*<dirección de correo>*; ruf=mailto:*<dirección de correo>*; fo=1; adkim=r; aspf=r; pct=100; rf=afrf; ri=86400; sp=reject;

Demostración:

Creación de registros en el DNS

Próximos pasos

Completen el proceso e implementen DMARC con p=none en sus organizaciones.

Nombre de registro: _dmarc

Valor: “v=DMARC1; p=none; rua=mailto:*<dirección de correo>*; ruf=mailto:*<dirección de correo>;*”

Y no duden en ponerse en contacto con nosotros siempre que lo necesiten: por correo electrónico, en nuestro foro (community.globalcyberalliance.org) o concertando una videoconferencia.

¿Preguntas?

¡Gracias!

Shehzad Mirza
gca-dmarc@globalcyberalliance.org
smirza@globalcyberalliance.org