GLOBAL CYBER ALLIANCE

Shehzad Mirza

Director de operaciones

smirza@globalcyberalliance.org

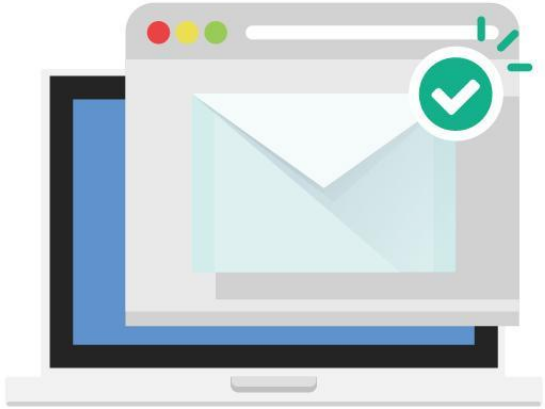
gca-dmarc@globalcyberalliance.org

Copyright © 2020 Global Cyber Alliance

Conceptos clave

Copyright © 2020 Global Cyber Alliance

LA SOLUCIÓN:



EFICACIA DEMOSTRADA PARA REDUCIR EL RIESGO DE SU CORREO ELECTRÓNICO

Protocolo DMARC de autenticación, notificación y validación
de mensajes de correo electrónico mediante nombres de dominio.
Funciona como un control de identidad con el nombre de dominio de su organización.

Copyright © 2020 Global Cyber Alliance

Otras ventajas de DMARC

- Protección de los consumidores de correo:
  - **Verificación DMARC, sin reglas**
  - El 80% del total de cuentas de correo electrónico en el mundo (fuente: Valimail)
- Mejoras en la entrega de correo
- Visibilidad: proporciona información sobre los intentos de spam, phishing e incluso spear phishing realizados en nombre de su organización

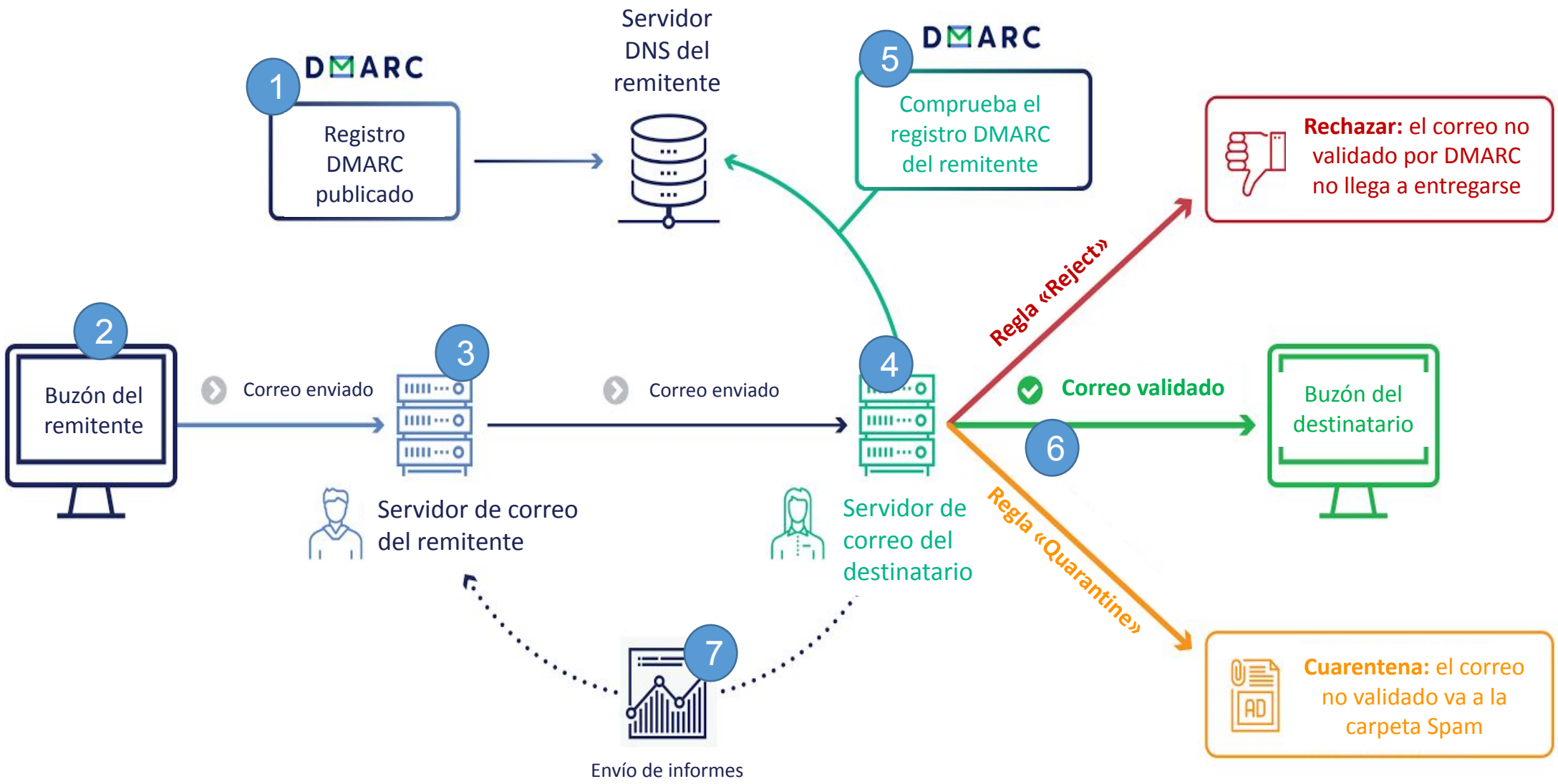
Copyright © 2020 Global Cyber Alliance

DMARC (sigue)

- Protege frente a la suplantación de dominios (persona@empresa.com)
- **Crea reglas para todos los dominios públicos**

Copyright © 2020 Global Cyber Alliance

Así funciona



Copyright © 2020 Global Cyber Alliance

Registro de texto en el DNS para DMARC

- Configuración básica:

  Host: _dmarc

  Valor: v=DMARC1; p=quarantine; **rua=mailto*:dmarc@gca-emailauth.org***; ruf=mailto*:<dirección de correo>;*

- Configuración compleja:

  Host: _dmarc

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

Copyright © 2020 Global Cyber Alliance

¿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

Copyright © 2020 Global Cyber Alliance

Implementación correcta

Los protocolos SPF (Sender Policy Framework, *convenio de remitentes* en español) y DKIM (DomainKeys Identified Mail, *correo identificado por DomainKeys*) son necesarios para que funcione DMARC:

- SPF se usa para definir los servidores autorizados para enviar correo
- DKIM se usa para añadir una firma digital, como capa extra para la autenticación de remitentes

Copyright © 2020 Global Cyber Alliance

SPF

- Recomendado: **–all** o **~all**
- Solo puede existir un registro
- SPF simplificado vs. dinámico (instantáneo)
  - Problema: límite de 10 dominios
- Alineación vs. verificación

Copyright © 2020 Global Cyber Alliance

Alineación SPF

Correcta:

From: info@globalcyberalliance.org

Return-Path: <info@globalcyberalliance.org>

Received-SPF: pass (google.com: domain of info@globalcyberalliance.org designates 2607:f8b0:4864:20::d34 as permitted sender) client-ip=2607:f8b0:4864:20::d34;

Fallida:

From: info@globalcyberalliance.org

Return-Path: < bounce-mc.us15_71628198.660451-8bd9e9bfe7@mail58.atl11.rsgsv.net >

Received-SPF: pass (google.com: domain of bounce-mc.us15_71628198.660451-8bd9e9bfe7@mail58.atl11.rsgsv.net designates 205.201.133.58 as permitted sender) client-ip=205.201.133.58;

Para que la alineación SPF sea correcta, el dominio del encabezado de remitente (From:) debe ser el mismo utilizado para la validación SPF (dominios de 'From:' y 'Return-Path' en el ejemplo).

Copyright © 2020 Global Cyber Alliance

DKIM

- Clave privada: debe protegerse
- Clave pública: para compartir
- Puede haber más de un registro
- CNAME o TXT
- Recomendado si se está usando un proveedor de servicios en la nube
- Alineación vs. verificación

Copyright © 2020 Global Cyber Alliance

Alineación DKIM

Correcta:

Encabezado del mensaje:

Desde: info@globalcyberalliance.org

Firma DKIM: v=1; a=rsa-sha256; c=relaxed/relaxed; d=globalcyberalliance.org; s=gca; h=mime-version:references:in-reply-to:from:date: message-id:subject:to :cc;

Fallida:

Encabezado del mensaje:

Desde: info@globalcyberalliance.org

Firma DKIM: v=1; a=rsa-sha256; c=relaxed/relaxed; d=mail8.mcsignup.com; s=default; h=mime-version:references:in-reply-to:from:date: message-id:subject:to :cc;

DKIM DMARC	DKIM solo	DKIM d=
alineado	valida	globalcyberalliance.org
no alineado	valida	mail9.mcsignup.com
alineado	valida	globalcyberalliance.org
alineado	valida	globalcyberalliance.org
alineado	valida	globalcyberalliance.org
no alineado	valida	mail13.mcsignup.com
no alineado	valida	mail8.mcsignup.com
no alineado	valida	gmail.mctxapp.net
no alineado	valida	mail10.mcsignup.com
no alineado	valida	gmail.mctxapp.net

Copyright © 2020 Global Cyber Alliance

Implementación en el DNS

DMARC

- Un registro por dominio

SPF

- Un registro por dominio
- **hostname** debe quedar como **@**, **null** o vacío

DKIM

- Varios registros por dominio
- Debe empezar por **<selector>._domainkey.**

Linux

- Comprobar **$ORIGIN <*dominio*>**
- Requiere comillas

Todos los DNS

- A veces no requieren nombres completos de dominio (FQDN)
- A veces no requieren comillas

Copyright © 2020 Global Cyber Alliance

Informes de DMARC

- DMARC genera dos tipos de informes:
  - Agregados (**rua**)
  - Forenses (**ruf**)
- Se envían en formato XML a la dirección que se indique (pueden ser varias)
- El número y la longitud de los informes dependerá de la cantidad de mensajes de correo electrónico que se envíen
- Ofrecen información sobre los mensajes marcados como sospechosos
- Permiten al personal técnico corregir posibles problemas con el bloqueo de mensajes válidos por las reglas

Copyright © 2020 Global Cyber Alliance

¿Y ahora qué?

- Revisar los informes:
  - Y ajustar SPF y DKIM según corresponda

- Aplicar **p=reject** a cualquier dominio público que no se use para correo

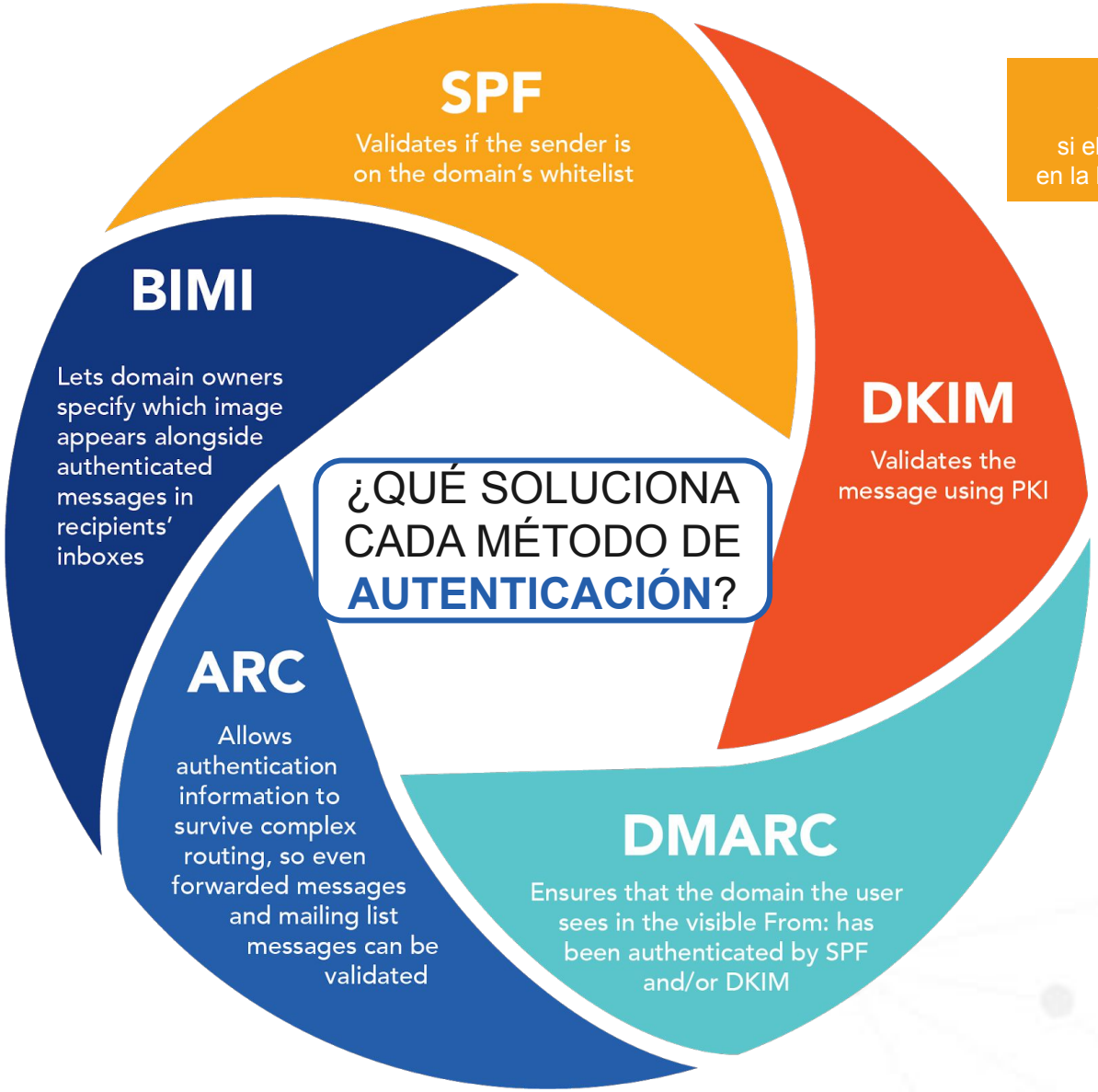
- Pasar a reglas estrictas (Quarantine/Reject)
  - Seguir revisando los informes
  - Ajustar SPF y DKIM según corresponda y siempre que se añadan nuevos sevicios de correo

- Aplicar mecanismos adicionales para la protección del correo electrónico

Copyright © 2020 Global Cyber Alliance

GLOBAL CYBER ALLIANCE

¿QUÉ SOLUCIONA CADA MÉTODO DE AUTENTICACIÓN?



SPF
Valida el mensaje si el emisor se encuentra en la lista blanca del dominio

DKIM
Valida el mensaje mediante una infraestructura de clave pública (PKI)

DMARC
Comprueba que el dominio mostrado en el campo visible De: (From:) haya sido autenticado por SPK o DKIM

BIMI
Permite a los titulares de los dominios indicar qué imagen debe aparecer junto a los mensajes validados en los buzones de entrada de los destinatarios

ARC
Conserva los datos de autenticación en procesos complejos de redirección, lo que facilita que los mensajes reenviados y las listas de distribución también puedan ser validados

Fuente: https://medium.com/@ykhan30/an-easy-win-for-email-security-2b84ac2a22da

Copyright © 2020 Global Cyber Alliance

ARC

- Siglas en inglés de *Authenticated Received Chain* (cadena de recepción autenticada)
- «Conserva los resultados de la autenticación de correo electrónico a través de cada uno de los intermediarios (*saltos*) que podrían llegar a modificar el mensaje»:
  - http://arc-spec.org
- Se utiliza en servicios de redirección de correo o en listas de distribución
- RFC 8617
- Herramientas: OpenARC (https://github.com/trusteddomainproject/OpenARC/releases)

Copyright © 2020 Global Cyber Alliance

BIMI

- Siglas en inglés de *Brand Indicators for Message Identification* (indicadores de marca para la identificación de mensajes)
- Requiere DMARC configurado de modo estricto (regla Reject o Quarantine)
- Registro de texto del DNS:

  Host: default._bimi.

  Valor: "v=BIMI1; l=<*ubicación del archivo de imagen*>; a=<*ubicación del archivo del certificado*>;"
- El archivo de imagen tiene que estar en formato SVG
- Referencias:
  - http://bimigroup.org/
  - https://bimi.agari.com/

Copyright © 2020 Global Cyber Alliance

DANE para SMTP

- Siglas en inglés de *DNS-Based Authentication of Named Entities* (autenticación de entidades mediante DNS)
- Establece conexiones TLS encriptadas sin las desventajas de STARTTLS
- Requiere un protocolo de seguridad de Internet para certificados digitales X.509
- Vinculado a nombres de dominio con extensiones de seguridad o DNSSEC (Domain Name System Security Extensions)
  - Ofrece una segunda fuente de verificación
- RFC 6698

Copyright © 2020 Global Cyber Alliance

DANE (sigue)

- Para tener en cuenta:
  - ¿Tiene DNSSEC su registrador de dominios?
  - ¿Tiene DNSSEC su servicio de correo electrónico en la nube?
  - Requiere crear registros DNS adecuados
- Aceptado por Microsoft

Copyright © 2020 Global Cyber Alliance

MTA-STS*

- Permite a los proveedores de servicios de correo recibir conexiones de SMTP protegidas con TLS
- Alojado en un servidor web con un nombre de host especial (requiere SSL)
- Permite a los dominios:
  - Optar por un mecanismo sólido de seguridad de la capa de transporte
  - Informar de forma segura sobre sus servidores MX
- RFC 8461

*Siglas en inglés de *Mail Transfer Agent-Strict Transport Security*
(agente de transferencia de correo-seguridad de transporte estricta)

Copyright © 2020 Global Cyber Alliance

MTA-STS (sigue)

Para tener en cuenta:

- Requiere un certificado SSL válido
- Requiere un registro de texto en el DNS válido:

  Nombre: _mta-sts

  Valor: “v=STSv1; id=20190423085700;”
- Debe crearse un archivo .txt con datos sobre el servidor MX:
  - Ubicación del archivo:

    https://mta-sts.domain.com/.well-known/mta-sts.txt
  - Utiliza TLS RPT para los informes
- Aceptado por Google

Copyright © 2020 Global Cyber Alliance

TLS RPT (informes de TLS)

- Modo de generación de informes que permite monitorizar el transporte seguro de correo electrónico a un dominio
- Solo requiere un registro de texto en el DNS:
  - _smtp._tls.*sudominio.com*. 300 IN TXT "v=TLSRPTv1;rua=mailto:tlsrpt@*sudominio.com*;"
- RFC 8460

Copyright © 2020 Global Cyber Alliance

Recursos

- **DMARC.org** (http://www.dmarc.org): gran fuente de información sobre DMARC
- **DMARC en la GCA:** https://dmarc.globalcyberalliance.org
- **Canal de YouTube de la GCA**
- **Foro de la comunidad de la GCA:** https://community.globalcyberalliance.org
- **Página de recursos del Bootcamp:** https://dmarc.globalcyberalliance.org/dmarc-bootcamp/

Copyright © 2020 Global Cyber Alliance

Últimos puntos

- Encuesta
- Certificado de asistencia

Copyright © 2020 Global Cyber Alliance

Proyectos de la GCA

- Cajas de herramientas de ciberseguridad (gcatoolkit.org):
  - Para pequeñas empresas
  - Para elecciones

- AIDE (gcaaide.org)

Copyright © 2020 Global Cyber Alliance

¿Preguntas?

Copyright © 2020 Global Cyber Alliance

¡Gracias!

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

Copyright © 2020 Global Cyber Alliance