CÓMO IMPLEMENTAR DMARC EN SU EMPRESA

Para que se pueda emitir un certificado de marca verificada (VMC) para una empresa, la organización debe cumplir con el protocolo de autenticación DMARC (autenticación de mensajes, informes y conformidad basada en dominios). En esta guía, explicamos los pasos que debe seguir para garantizar que su empresa haya implementado DMARC correctamente.

digicert®

digicert®

¿QUÉ ES DMARC?

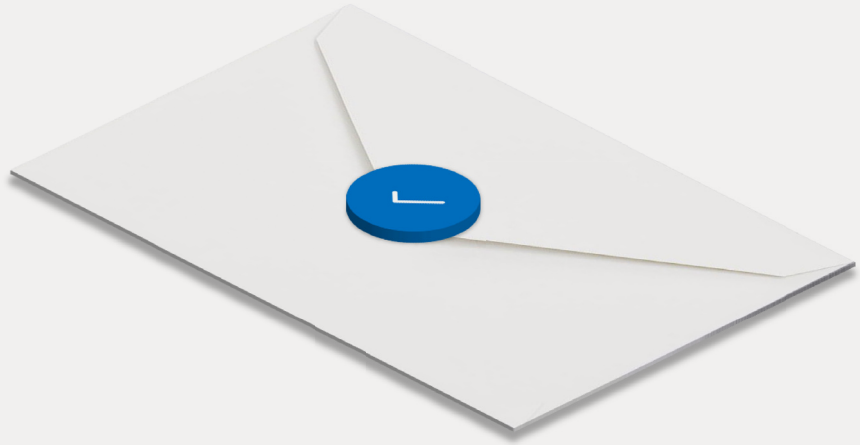
DMARC es un protocolo de autenticación de correo electrónico, políticas e informes que permite a las empresas proteger su dominio de usos no autorizados, como la usurpación y los ataques de phishing.

A continuación ofrecemos un resumen básico:

- DMARC es un registro TXT almacenado en el DNS que permite a los destinatarios comprobar la autenticidad de los correos electrónicos que reciben.
- Está diseñado para poder integrarse en el proceso de autenticación de correo entrante que ya utilice la empresa y ayuda a los destinatarios a decidir si un mensaje determinado se corresponde o no con lo que saben del remitente.
- Las empresas pueden elegir una de estas tres políticas para lidiar con los mensajes que no se correspondan con lo anterior:

- «p = none» (nada; ninguna acción)
- «p = quarantine» (poner en cuarentena)
- «p = reject» (rechazar)

- Para que DMARC funcione correctamente, es necesario configurar previamente los protocolos SPF (Sender Policy Framework o convenio de remitentes) y DKIM (Domain Keys Identified Mail o correo identificado por clave de dominio).
- Se puede consultar el registro DMARC de una empresa mediante «herramientas» basadas en Internet, como esta de valimail.com.



MEJORAR LA AUTENTICACIÓN DEL CORREO ELECTRÓNICO PASA POR IMPLEMENTAR DMARC

El objetivo de DMARC es establecer un sistema de emisores y receptores que colaboren de cara a mejorar las prácticas de autenticación de correo que emplean los remitentes y permitir que los destinatarios rechacen aquellos mensajes que no hayan sido autenticados.

digicert®

¿POR QUÉ IMPLEMENTAR DMARC?

La implementación de DMARC les ofrece a las empresas cuatro ventajas principales:

1. **Seguridad**

   Proteja a los usuarios del correo no deseado, el fraude y el phishing bloqueando cualquier uso no autorizado de su dominio de correo electrónico.

2. **Visibilidad**

   Obtenga informes detallados sobre quién (o qué) envía correos electrónicos utilizando su dominio.

3. **Entrega**

   Aumente las tasas de entrega entre un 5 y un 10 % y evite que sus mensajes acaben marcados como correo no deseado.

4. **Protección de la marca**

   Proteja su marca de los ataques de suplantación de identidad.

Porcentaje de clientes que se muestran reacios a establecer relaciones con una marca tras haber sufrido un ataque de phishing que se hacía pasar por esa empresa.

digicert®

CÓMO CONFIGURAR SPF:

1. Recopile todas las direcciones IP que se utilizan para enviar correos electrónicos desde su dominio. Por ejemplo:
    - Servidor web
    - Servidor de correo de la oficina
    - Servidor de correo del proveedor de servicios de Internet
    - Cualquier servidor de correo de terceros
2. Confeccione una lista de sus dominios (sean o no de envío).
3. Para cada dominio, elabore un registro SPF en formato .txt utilizando un programa de edición de textos (p. ej., Notepad++, Vim o Nano).

    Ejemplo 1: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 ip4:x.x.x.x -todos
    Ejemplo 2: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 incluir:terceros.com -todos
4. Publique su registro SPF en el DNS.

    Si es usted quien gestiona su DNS, simplemente deberá agregar un registro TXT nuevo que contenga el texto SPF. En caso contrario, póngase en contacto con el administrador de su servidor para que agregue el registro.
5. Una vez que se haya agregado el registro al DNS, verifíquelo con una herramienta de comprobación de SPF.

¿QUÉ ES SPF?

No permita que un remitente no autorizado manche su reputación

El protocolo SPF acuñó el concepto de autenticación del correo basada en dominios. Previene la suplantación de identidad, ya que permite a los propietarios de un dominio aprobar automáticamente las direcciones IP de los servidores que tienen autorización para enviar correos en nombre de dicho dominio. Si un servidor de correo con una dirección IP que no figura en la lista intenta enviar un correo electrónico utilizando ese dominio, no superará la autenticación SPF.

digicert®

CÓMO CONFIGURAR DKIM:

1. Elija un selector DKIM.

Este debería ser una secuencia de texto sencilla definida por el usuario, que se agregará al nombre del dominio para ayudar a identificar la clave pública DKIM (p. ej., «estándar»).

Ejemplo: «estándar._dominio.ejemplo.com» = nombre del host

2. Genere un par de claves (una privada y otra pública) para su dominio.

- Los usuarios de Windows pueden utilizar PuTTYgen
- Los usuarios de Linux y Mac pueden utilizar ssh-keygen

3. Elabore y publique un registro TXT nuevo.

Elabore un registro nuevo en su consola de gestión de DNS utilizando la clave pública del par generado en el paso anterior.

Ejemplo: v=DKIM1; p=SuClavePública

¿QUÉ ES DKIM?

Evite la manipulación de los correos mientras se transfieren

DKIM es un estándar de autenticación de correo electrónico que se sirve de la criptografía de clave pública y privada para firmar mensajes de correo electrónico.

DKIM se utiliza para verificar que el correo procede del dominio al cual está asociada la clave DKIM y que no ha sido alterado en tránsito.

CONFIGURACIÓN DE DMARC EN EL MODO DE SUPERVISIÓN

1. Asegúrese de haber configurado correctamente los protocolos SPF y DKIM.

2. Elabore un registro de DNS.

   El nombre del registro DMARC en formato .txt debería ser similar a «_dmarc.su_dominio.com».

   Ejemplo: «v=DMARC1;p=none; rua=mailto:informesdmarc@su_dominio.com»

   Si es usted quien gestiona su DNS, cree un registro DMARC con el valor «p=none» (modo de supervisión) del mismo modo en que elaboró los registros SPF y DKIM.

   Si no gestiona usted el DNS, pídale a su proveedor de DNS que elabore el registro DMARC.

3. Verifique su registro DMARC mediante una herramienta de comprobación de DMARC.

   Nota: Normalmente, hay que esperar entre 24 y 48 horas para repetir la operación.

digicert®

¿QUÉ ES EL MODO DE SUPERVISIÓN DE DMARC?

Obtenga una mayor visibilidad de aquello que se envía desde su dominio

En el modo de supervisión, los propietarios de un dominio pueden revisar los informes DMARC que contienen el tráfico de correo electrónico para dicho dominio.

Los informes señalan aquellos mensajes que puede que no lleguen a entregarse porque se pondrán en cuarentena, o bien porque serán rechazados una vez que se esté utilizando la configuración más estricta de DMARC. Además, los informes DMARC ofrecen información sobre todos los sistemas y servicios que envían correos electrónicos desde el dominio que se está supervisando.

NOTA: En el modo de supervisión, no se toma ningún tipo de acción. Aquellos correos que no superen la autenticación se entregarán con normalidad, lo que le permite evitar posibles interrupciones al implementar DMARC.

digicert®

ETIQUETAS HABITUALES EN LOS REGISTROS DMARC EN .TXT

NOMBRE DE LA ETIQUETA	¿ES OBLIGATORIA?	FUNCIÓN
V	SÍ	VERSIÓN DEL PROTOCOLO
P	SÍ	VERSIÓN DEL POLÍTICA
PCT	NO	PORCENTAJE DE CORREOS SOMETIDOS A FILTRADO
RUA	NO	URI A LA QUE SE DEBE ENVIAR EL INFORME GLOBAL
SP	NO	POLÍTICA PARA LOS SUBDOMINIOS DEL DOMINIO

digicert®

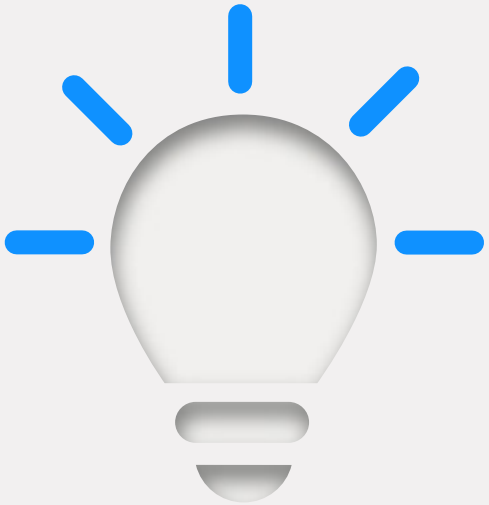
¿QUÉ INFORMACIÓN OFRECE EL INFORME DMARC?

El informe dice a los propietarios de los dominios cuántos mensajes fraudulentos utilizan su dominio, de dónde proceden y si serían o no bloqueados por una política DMARC con el valor «quaratine» (poner en cuarentena) o «reject» (rechazar).

El informe de cada receptor es un archivo XML que incluye los siguientes campos:

- Recuento de los mensajes procedentes de cada una de las direcciones IP
- Qué se hizo con esos mensajes de acuerdo con la política DMARC mostrada
- Resultados SPF para esos mensajes
- Resultados DKIM para esos mensajes

El informe XML se puede leer, pero no resulta cómodo. Por tanto, puede ser recomendable recurrir a un procesador de informes DMARC, como Valimail o algún otro proveedor de servicios DMARC.



CUATRO UTILIDADES DE LOS INFORMES DMARC

Establezca un buen punto de partida antes de empezar a aplicar las políticas

1. Identifique el tráfico marcado como no legítimo.

2. Compruebe si DMARC ha marcado algún correo electrónico legítimo como no legítimo. Una vez configurada la aplicación de políticas, esos correos serían rechazados o puestos en cuarentena, dependiendo de la política aplicada.

3. Póngase en contacto con los posibles propietarios de los sistemas o aplicaciones para aclarar que los correos que se están marcando como no legítimos son en realidad legítimos.

4. De ser necesario, actualice su registro SPF agregando a la lista de permitidos las direcciones IP que son legítimas pero que no figuraban en ella.

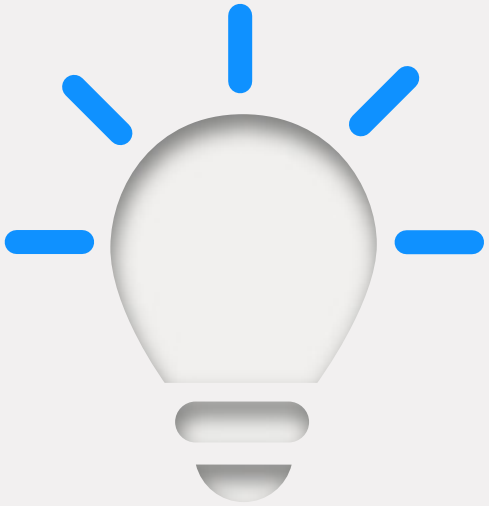
digicert®

UTILICE LOS INFORMES DMARC PARA PONER TODO EN ORDEN ANTES DE ACTIVAR LA APLICACIÓN DE POLÍTICAS

Analizar los informes DMARC lleva tiempo, pero más llevaría solucionar los problemas que pueden surgir si los propietarios de los dominios pasan por alto o identifican mal a los emisores de los correos, ya que algunos mensajes «buenos» podrían acabar bloqueados una vez activa la aplicación de políticas DMARC («poner en cuarentena» o «rechazar»), lo que entorpecería, además, sus progresos.

Para evitarlo, le recomendamos que tome las siguientes medidas internas antes de activar la aplicación de políticas DMARC:

- Haga un inventario de todos los emisores de correo identificados en el informe DMARC, además de otros que hayan podido mencionar las partes interesadas.
- Identifique a los propietarios de cada servicio o emisor de correo.
- Clasifique los servicios de envío como autorizado, no autorizado o malicioso.
- Con la ayuda de las demás partes interesadas, identifique a cualquier otro emisor que pueda no figurar en el informe DMARC.
- Ponga en conocimiento de las partes interesadas cada emisor nuevo que identifique.
- Actualice su registro SPF para incluir todas las direcciones IP de los emisores de correo legítimos que vaya encontrando.



RECOMENDACIONES PARA LA COMUNICACIÓN PREVIA A LA APLICACIÓN DE POLÍTICAS

Cinco consejos para mejorar la adopción

- Documente una política de implementación que pueda compartir con las demás partes interesadas.
- Póngase en contacto con un proveedor de asistencia para DMARC, como Valimail, si las tareas relativas a este protocolo le resultan demasiado abrumadoras o si necesita ayuda.
- Comparta las conclusiones de los informes DMARC tan pronto como estén disponibles.
- Inicie la implementación de DMARC como un proyecto interno.
- Convierta a sus directivos en los principales patrocinadores del proyecto.

¿DURANTE CUÁNTO TIEMPO DEBERÍA PERMANECER DMARC EN EL MODO DE SUPERVISIÓN?

El tiempo variará en función de la empresa: normalmente, las grandes empresas necesitarán más que las pymes. Le recomendamos que cuente con unas cuantas semanas o unos cuantos meses.

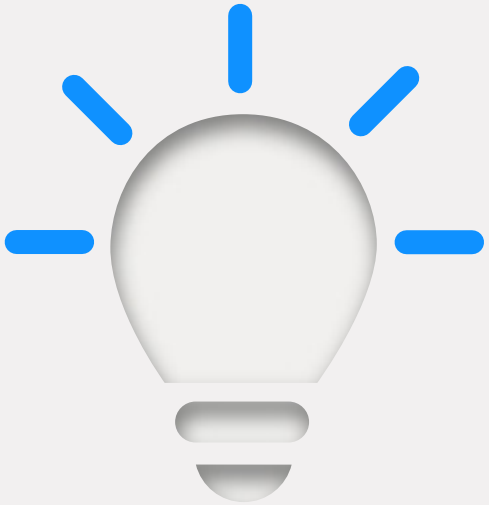
Cuando tenga la certeza de que su inventario es exhaustivo, todos los emisores autorizados han sido identificados y su empresa cuenta con información suficiente, podrá pasar a la fase «poner en cuarentena».

En el modo «quarantine», se pondrán en cuarentena los mensajes que no superen la autenticación. Por lo general, esto significa que se enviarán a la carpeta de correo no deseado del usuario.

CÓMO CONFIGURAR LA POLÍTICA DMARC EN MODO «QUARANTINE»

1. Inicie sesión en su servidor DNS y busque el registro DMARC.
2. Abra el registro DMARC para el dominio en cuestión y cambie la política de «p=none» a «p=quarantine».
   Ejemplo:
   "v=DMARC;p=quarantine;pct=10;rua=mailto:informesdmarc@su_dominio.com"
3. Agregue la etiqueta «pct» (porcentaje de correos sometidos a filtrado). Recomendamos empezar con el 10 %.
4. A medida que vaya ganando confianza, incremente el porcentaje de mensajes filtrados de forma gradual hasta «pct=100» (100 %).

   NOTA: Para cumplir con los estándares de BIMI y VMC, debe haber alcanzado «pct=100», pero la política puede ser «quarantine» (poner en cuarentena) o «reject» (rechazar).



¿CÓMO FUNCIONAN LAS ETIQUETAS?

- Si se especifica una política distinta de «p=none», dicha política se aplicará al porcentaje que figura en la etiqueta «pct».
- Para el porcentaje restante, se aplicará la siguiente política menos restrictiva (p. ej., si en un registro DMARC tenemos «p=quarantine» y «pct=10», el 10 % del tráfico que no supere la autenticación será puesto en cuarentena, y el 90 % restante se enviará con normalidad).

digicert®

UNA VEZ ALCANZADO EL FILTRADO DEL 100 % DE LOS CORREOS, PODRÁ PASAR A «P=REJECT», LA POLÍTICA MÁS ESTRICTA.

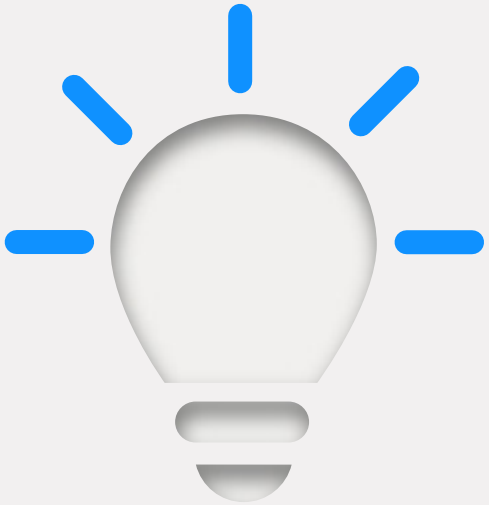
CÓMO CONFIGURAR LA POLÍTICA DMARC EN MODO «REJECT»

1. Abra el registro DMARC a través de su consola de DNS.
2. Cambie «p=quarantine» por «p=reject».
   Ejemplo: "v=DMARC;p=reject;pct=100;rua=mailto:informesdmarc @ su_dominio.com
3. Guarde el registro.

CONSEJO: Durante esta fase, es muy importante continuar con la supervisión para garantizar que no se rechacen y se eliminen correos electrónicos legítimos.

¿Tiene más preguntas? Envíenos un correo electrónico hoy a contactus@digicert.com o visítenos en https://www.digicert.com/es/tls-ssl/verified-mark-certificates/

digicert®



¿QUÉ PASA CON LOS CORREOS BAJO LA POLÍTICA «REJECT»?

Se bloqueará o eliminará cualquier mensaje que no supere la comprobación DMARC (correo no autorizado), y el destinatario nunca lo recibirá ni sabrá que ha sido eliminado.