digicert®

# CERTIFICADOS DE MARCA VERIFICADA

## Deje su marca en el marketing por correo electrónico y saque a relucir la seguridad de su identidad

Todos utilizamos el correo electrónico a diario. Eso es lo que lo vuelve sumamente útil y particularmente vulnerable a los ataques, en especial a los que están relacionados con la identidad, como el phishing. De hecho, el 96 % de los ataques de phishing se realizan por correo electrónico y, en 2020, el 75 % de las empresas multinacionales se convirtieron en el blanco de esos ataques.

¿Por qué? En gran parte, porque las empresas no contaban con un proceso eficaz para identificarse ante los usuarios de manera concreta e instantánea ni tenían un método confiable para detectar y aislar rápidamente el contenido malicioso que se hiciera pasar por mensajes legítimos.

Los certificados de marca verificada (VMC, por sus siglas en inglés), junto con el método BIMI y el protocolo DMARC, cambian toda esa dinámica, ya que ofrecen un nuevo enfoque sumamente visual para la promoción de la marca y medidas de prevención de phishing que ayudan a proteger a los consumidores y las empresas de los ataques relacionados con la identidad.

## ¿Cómo funciona el correo electrónico verificado?

### Protocolo DMARC + BIMI + VMC = Correo electrónico con logotipo verificado

#### ¿Qué son los certificados VMC?

Los certificados VMC son un tipo de certificado nuevo e innovador que permite a las empresas mostrar un logotipo de marca certificado junto al campo «Remitente» en la bandeja de entrada de sus clientes, incluso antes de que estos abran el mensaje. Si compra un certificado VMC, DigiCert validará su identidad por completo e incluso comprobará que su logotipo esté oficialmente registrado.

Consulte esta lista aprobada de oficinas de marcas comerciales para el registro de los certificados VMC.

#### ¿Qué es DMARC?

DMARC, la autenticación de mensajes, informes y conformidad basada en dominios, es una política de autenticación de correo electrónico que se basa en los protocolos SPF y DKIM, pero que, además, vincula al autor, a las políticas publicadas que atañen al manejo de los errores de autenticación por parte de los destinarios y al envío de informes de los destinatarios a los remitentes, con el fin de mejorar la visibilidad y proteger más el dominio frente a los ataques de phishing y suplantación de identidad.

Descargue nuestra guía detallada para la implementación del protocolo DMARC.

#### ¿Qué es BIMI?

BIMI, que son las siglas en inglés de «indicadores de marca para la identificación de mensajes», es una especificación de correo electrónico que permite mostrar logotipos de marca en los clientes de correo compatibles para fomentar la adopción masiva del protocolo DMARC.

#### ¿Cómo funcionan juntos?

El cliente de correo electrónico valida que su empresa cumpla el protocolo DMARC por medio de la confirmación de su registro BIMI y del logotipo respaldado por el certificado VMC. Si la verificación arroja resultados positivos, se mostrará su logotipo, lo que señala visualmente que sus mensajes son auténticos, aumenta las interacciones e impulsa el reconocimiento de la marca.


Se envía el correo electrónico

Se verifica la dirección IP del remitente en la lista de entidades permitidas de SPF

Se verifica la firma de correo electrónico del remitente con DKIM

Se reciben únicamente los correos electrónicos verificados

## Ventajas para los equipos de TI

### El protocolo DMARC ofrece mayor visibilidad, seguridad y control

- Refuerce la seguridad mediante la implementación del protocolo DMARC.
- Reduzca el riesgo de que usted y su marca sufran un ataque de phishing.
- Obtenga mayor visibilidad y control de los mensajes que envía y recibe su dominio.
- Acceda a datos precisos sobre los tipos de ataques que recibe su marca y la frecuencia de esos embates.
- Asegúrese de que los correos electrónicos legítimos se entreguen de forma confiable y se puedan identificar con facilidad.

## Ventajas para los especialistas en marketing

### Conquiste las bandejas de entrada

- Mejore las interacciones en más de un 10 %[1].
- Impulse el reconocimiento de la marca con cada mensaje que envíe.
- Logre que su marca sea sinónimo de cumplimiento del protocolo DMARC y de mayor seguridad en materia de correos electrónicos.
- Ofrezca una experiencia de marca más destacada, auténtica y confiable.
- Diferencie visualmente sus mensajes en el canal de comunicación más eficaz y popular.

## Ventajas para los consumidores

### Menos ataques de phishing es sinónimo de más confianza

Dado que cada vez más marcas adoptan DMARC, cabe esperar que se reduzca la cantidad de mensajes de phishing que llegan a las casillas de los consumidores, lo que se traduce en menos riesgos, bandejas de entrada menos llenas y, en resumidas cuentas, una experiencia de usuario mejorada.

## Requisitos para la validación

Para obtener un certificado VMC, las empresas deben llevar a cabo una serie de procedimientos de validación similares a los que se necesitan para obtener un certificado SSL con EV. Durante el proceso, se debe validar la identidad de un individuo y, además, un notario o un abogado deben realizar la comprobación cara a cara. Asimismo, el equipo de validación de DigiCert realizará una videollamada con el solicitante en la que este deberá mostrar su documento de identidad frente a la cámara. Por último, DigiCert también tiene que validar que el logotipo esté oficial y legalmente registrado y que tenga el formato adecuado.

Descubra cómo convertir el logotipo al formato SVG adecuado.

## Compra del certificado VMC

Los certificados VMC se pueden comprar en CertCentral.

Nota: Para completar la compra, deberá tener una cuenta activa.

Comprar ahora

## Instalación

1. Una vez que haya enviado a DigiCert el archivo SVG con el logotipo, recibirá un archivo con una cadena de certificados con cifrado PEM.

2. Tanto el archivo SVG como el de la cadena de certificados se deben ubicar en un servidor de acceso público y se debe poder acceder a ellos con HTTPS, ya que HTTP generará fallas.

3. Luego, deberá actualizar su registro BIMI con la URL y la ubicación del archivo correctas.

# Preguntas frecuentes

**¿Cuántos certificados VMC voy a necesitar?**

Por lo general, depende de la cantidad de logotipos que su empresa tenga en uso. Lea nuestra publicación de blog para obtener más información.

**¿Puedo usar una marca denominativa en lugar del logotipo?**

Sí, puede optar por usar una marca denominativa en lugar del logotipo, pero esta debe estar registrada en una agencia de marcas comerciales pertinente.

**¿Cómo puedo saber si mi empresa cumple el protocolo DMARC?**

Si quiere saber si su empresa cumple el protocolo DMARC, haga clic aquí.

**¿Cómo puedo consultar si mi logotipo está registrado y dónde puedo obtener la aprobación?**

El logotipo debe estar registrado en una oficina de marcas comerciales autorizada.

Lea nuestra publicación de blog para obtener más información sobre el proceso de registro.

**¿Qué clientes de correo electrónico muestran los certificados VMC?**

Gmail, Yahoo!, Fastmail, Verizon y muchos más.

La lista de clientes compatibles va a seguir creciendo, ya que los certificados VMC son algo sumamente nuevo. Visite nuestro sitio web para consultar la lista más actualizada.

**¿Qué pasa si dejo de cumplir el protocolo DMARC luego de comprar un certificado VMC?**

El certificado seguirá siendo válido, pero no se mostrará el logotipo. Si desea que el logotipo siga apareciendo, debe cumplir activamente el protocolo DMARC, lo cual se ve reflejado en su registro BIMI.

**¿Con qué frecuencia debo renovar el certificado y revalidar mi identidad?**

Los clientes deben renovar el certificado anualmente. Una vez que un cliente haya validado su empresa, no tendrá que volver a someterse al proceso de certificación notarial, pero sí tendrá que revalidar su identidad cada 398 días, de forma similar a lo que sucede con los certificados TLS/SSL con EV estándar, y deberá acceder a CertCentral para renovar el certificado.

**Somos una empresa oficial, pero nuestro logotipo no está registrado. ¿Podemos usar un certificado VMC?**

Por el momento, no. Solo se muestran los certificados que están oficialmente registrados.

**¿Tiene alguna otra pregunta?**

Obtenga más información y póngase en contacto en https://www.digicert.com/es/tls-ssl/verified-mark-certificates