— PROPIEDAD INTELECTUAL

Indicadores de marca para la identificación de mensajes

Lo más nuevo en servicios de autenticación.

por Miguel Ángel Carpio y Emiliano Vargas

EN RESUMEN

El incremento de ciberataques como el phishing y el fraude por correo electrónico corporativo exige robustecer la seguridad en las comunicaciones digitales. El estándar BIMI permite desplegar el logotipo de una marca en la bandeja de entrada tras validar los protocolos SPF, DKIM y DMARC, junto con un certificado digital de marca emitido por una entidad verificadora. Este análisis examina la operatividad de los certificados VMC y CMC, el reconocimiento directo de registros marcarios del IMPI para México y el paralelismo funcional de este mecanismo técnico con la marca de certificación en el derecho de propiedad industrial mexicano.

A la par del progreso que se presenta en materia de la digitalización de las comunicaciones, crece también la necesidad de proteger no solo la información que nuestros servicios de mensajería contienen, sino también a quienes compartimos esa información, pues, la naturaleza propia de este tipo de comunicaciones permite a cualquier persona aprovechar la imagen de una marca haciéndose pasar por ella al momento de hacer uso de estos servicios.

Esta conducta se conoce como “phishing”, es decir, una estafa consistente en suplantar la identidad de una empresa o institución reconocida para obtener datos personales o información bancaria de la víctima. Es tan común que incluso grandes corporativos han resultado afectados. Tal es el caso de Sony Pictures, cuyos empleados recibieron correos que simulaban ser avisos de verificación de Apple ID, lo cual derivó en la filtración de más de 100 terabytes de información confidencial y en pérdidas millonarias.

Otro caso de especial relevancia es el que sufrieron Facebook y Google bajo la modalidad conocida como Business Email Compromise. El atacante envió correos fraudulentos a diversos empleados de ambas empresas haciéndose pasar por un fabricante de equipo de cómputo y llegó incluso a registrar un dominio de internet para dar confiabilidad al engaño, con el objeto de solicitar el pago de facturas por supuestos servicios. Durante dos años, el perpetrador obtuvo por esta vía cuantiosos pagos de ambas empresas.

© 2026 ECIJA México · Todos los derechos reservados

Ejemplos como los anteriores evidencian el peligro que estas conductas representan tanto para la reputación de la marca falsificada como para el receptor de dichos mensajes. En atención a este y otros riesgos que la comunicación digital representa, surgen los **indicadores de marca para la identificación de mensajes**, o **BIMI** por sus siglas en inglés (Brand Indicators for Message Identification), el cual es, en síntesis, una especificación de correo electrónico que permite mostrar el logotipo de una marca al costado de un correo enviado desde su dominio, funcionando así como un autenticador, además de tener un beneficio publicitario inherente por la exposición visual que el propio servicio genera.

Ahora bien, BIMI no autentica por sí mismo los mensajes; es el indicador de que el remitente cumple con los protocolos de autenticación necesarios. Tampoco es BIMI quien revisa el derecho sobre el logotipo: esa función corresponde a una autoridad verificadora de marcas (Mark Verifying Authority), entidad certificadora que emite el certificado digital conforme a los requisitos del AuthIndicators Working Group. Superadas ambas verificaciones, el logotipo opera como un "sello de autenticidad", si bien su despliegue —y el de indicadores adicionales, como una "palomita azul" similar a la de Instagram o X— depende, en último término, de cada proveedor de correo.

Para entender cómo se genera la protección antes mencionada, conviene señalar que BIMI funciona como una cadena en la que cada uno de sus eslabones cumple con una parte fundamental para verificar que el origen del mensaje es seguro, partiendo por la autenticación en sí misma, la cual se otorga, tras cumplir con los protocolos **SPF**, **DKIM** y **DMARC**.

Cada protocolo verifica un aspecto distinto: SPF, que el servidor de origen está autorizado por el dominio remitente; DKIM, que el mensaje salió de ese dominio y no fue alterado, y DMARC, que el dominio autenticado coincide con el que ve el destinatario. Se trata, en pocas palabras, del filtro que depura aquellos correos que provienen de servidores seguros, de aquellos que tienen un origen desconocido, otorgando una barrera adicional de protección en las comunicaciones por correo. Cabe precisar que estos protocolos únicamente autentican el dominio del que proviene el correo, sin acreditar por sí mismos que el remitente tenga derecho a usar el logotipo que se muestra; esa verificación corresponde al certificado digital de marca, como se explica a continuación.

Posteriormente, una vez cumplidos los requisitos de protocolo, el titular del dominio debe obtener un certificado digital de marca, que acredita su derecho al uso del logotipo, ya sea por un título de registro de marca o por el uso continuado, pues BIMI admite dos vías para asegurar que la marca a incluir en el autenticador es por su parte segura:

- Certificado de marca verificada (VMC): exige que la marca cuente con un registro vigente ante una oficina de marcas reconocida por la Organización Mundial de la Propiedad Intelectual (OMPI), y es el único que permite que algunos proveedores, como Gmail, muestren la "palomita azul" junto al logotipo.
- Certificado de marca común (CMC): Elimina el requisito de registro marcario y determina que basta con probar el uso continuado de la marca por 12 meses, acreditando un derecho de uso invocado por el solicitante bajo common law o su equivalente en sistemas de derecho civil. En el derecho mexicano, el derecho nace del registro, por lo que, el CMC es tan solo una prueba de uso y no reconoce de ningún modo un derecho marcario.

De lo anterior se desprende una buena noticia para los titulares de marcas mexicanas. La versión vigente de los requisitos del AuthIndicators Working Group (1.8, de junio de 2026) define a la oficina de marcas por referencia a las reconocidas por la OMPI, sin limitarla ya a un listado cerrado, por lo que el registro otorgado por el Instituto Mexicano de la Propiedad Industrial

© 2026 ECIJA México · Todos los derechos reservados

("IMPI") basta para solicitar el VMC, sin necesidad de acudir a oficinas extranjeras o al Protocolo de Madrid. Con todo, conviene confirmar previamente que la autoridad verificadora elegida ya acepta registros mexicanos, pues en la práctica algunas pueden mantener listados más restringidos.

Finalmente, vale la pena analizar BIMI desde la óptica del derecho de propiedad industrial mexicano y la figura de la marca de certificación. Ambas cumplen una función similar, pues existen para informar al público consumidor que un tercero independiente verificó aquello que el destinatario no está en posibilidad de comprobar por sí mismo, y comparten también una estructura triangular en la que quien certifica no es quien ostenta el signo, ya que la autoridad verificadora verifica la existencia legal, física y operativa del remitente, así como su titularidad sobre el logotipo, pero no participa en el envío de los correos, del mismo modo que el titular de una marca de certificación no puede desarrollar la actividad que certifica.

A ello se suma que los requisitos emitidos por el AuthIndicators Working Group operan como un equivalente funcional de las reglas de uso que acompañan a esta clase de signos, al definir las características verificadas, el método de comprobación y las condiciones bajo las cuales el certificado puede utilizarse o revocarse, ya sea por la caducidad o nulidad de la marca, o bien por resolución firme de un tribunal u oficina marcaria que declare la existencia de una infracción. Con todo, la comparación es únicamente funcional y no supone una equivalencia jurídica: el logotipo que se despliega mediante BIMI no es una marca de certificación en términos de la Ley Federal de Protección a la Propiedad Industrial, ni la autoridad verificadora es titular de un signo de esa naturaleza; se trata de un esquema técnico, privado y voluntario, cuya eficacia depende de los proveedores de correo que lo adoptan.

BIMI representa un avance importante en materia de autenticación de las comunicaciones digitales, pues materializa una verificación que hasta ahora ocurría únicamente entre servidores y, al condicionar el despliegue del logotipo al cumplimiento de los protocolos de autenticación, incentiva la adopción de medidas de seguridad que benefician tanto al titular de la marca como al destinatario del mensaje.

En el caso de México, al bastar un registro ante el IMPI para solicitar el VMC, BIMI se suma a los incentivos para registrar no solo la denominación de una marca, sino también el logotipo con el que la empresa se identifica en sus comunicaciones digitales.

— CONTACTOS



Miguel Ángel Carpio Pertierra
Partner
Propiedad Intelectual
macarpio@ecija.com



Emiliano Vargas Fernández
Professional Legal Support
Propiedad Intelectual
evargas@ecija.com

© 2026 ECIJA México · Todos los derechos reservados

Propiedad Intelectual · info@ecija.com · T +52 55 5662 6840

La información contenida en este documento es de carácter general y meramente informativa. No constituye asesoría legal sobre asuntos específicos y no debe utilizarse como sustituto de la consulta con un asesor legal calificado. Para asuntos específicos, le invitamos a contactar a nuestros profesionales.

© 2026 ECIJA México · Todos los derechos reservados