



13 años

www.seguridadamerica.com

WEBINAR EDUCATIVO GLOBALSIGN

S/MIME: Cifrado y Firma digital para correos críticos

Cómo proteger comunicaciones sensibles y apoyar el cumplimiento de las Leyes 21.663 y 21.719.

VMC/CMC

Certificados que validan tu marca y muestran tu logo como remitente verificado y confiable en el correo.

Diego López | Seguridad América
Antonio Gutiérrez | GlobalSign



Lo que aprenderá en esta sesión

Proteger comunicaciones, controlar exposición y demostrar medidas de seguridad.



SEGURIDAD AMÉRICA.COM
Fortaleciendo Internet



GlobalSign®
by GMO

01 Correo y cumplimiento

¿Por qué el correo debe formar parte de la estrategia de protección de datos?

02 S/MIME en simple

¿Qué es, cómo funciona y qué protege en mensajes y adjuntos?

03 Firma vs Cifrado

Diferencias prácticas entre validar origen e impedir lectura no autorizada.

04 Leyes 21.719 y 21.663

¿Cómo S/MIME apoya controles técnicos sin reemplazar el cumplimiento integral?

05 Implementación corporativa

¿Cómo administrar certificados S/MIME de forma centralizada con GlobalSign?

06 VMC/CMC

Identidad visual de marca en bandejas compatibles mediante BIML.



El correo también debe entrar en la estrategia de protección de datos

- Los riesgos no están sólo en bases de datos: también viven en adjuntos, reenvíos y cadenas de correo.
- La protección de datos exige controles proporcionales al riesgo y capacidad de demostrar medidas adoptadas.
- El correo debe conectarse con clasificación de información, DLP, IAM, retención y respuesta a incidentes.

No basta proteger el servidor: hay que proteger el contenido y la identidad que viajan en el mensaje.



S/MIME: CERTIFICADOS DIGITALES APLICADOS AL CORREO

Secure/Multipurpose Internet Mail Extensions usa PKI para firmar y cifrar mensajes MIME

1. CERTIFICADO

- Identidad digital asociada a usuario o casilla.



2. PROTEGER

- Firma o cifrado según política y riesgo.



3. VALIDAR

- El receptor verifica origen, integridad o descifra.

S/MIME protege el mensaje, no sólo la conexión que lo transporta.



02 S/MIME en simple



SEGURIDAD AMÉRICA.COM
Fortaleciendo Internet



GlobalSign®
by GMO

S/MIME

GlobalSign

Fabian Vidal - Seguridad America

Marketing - Seguridad America

Firmado por: fvidal@seguridadamerica.com

Propuesta S-MIME 2025_.pdf
Archivo .pdf

Estimado equipo de Marketing,

Junto con saludar, se adjunta brochure de GlobalSign.

Saludos,

Firma digital: válida

Asunto: GlobalSign

De: Fabian Vidal - Seguridad America

Firmado por: fvidal@seguridadamerica.com

La firma digital de este mensaje es válida y de confianza.

Para obtener más información acerca del certificado utilizado para firmar el mensaje digitalmente, haga clic en Detalles.

Detalles...

Cerrar

☐ Avisar sobre los errores del correo firmado digitalmente antes de abrir mensaje.

03 Firma vs Cifrado



SEGURIDAD AMÉRICA.COM
Fortaleciendo Internet



GlobalSign®
by GMO

Validar origen no es lo mismo que impedir lectura

Firma y cifrado se complementan, pero responden a riesgos distintos.

FIRMA DIGITAL

- Asocia una identidad verificada al mensaje.
- Detecta alteraciones posteriores.
- El contenido puede seguir siendo legible para destinatarios.

CIFRADO

- Usa la clave pública del destinatario.
- Mensaje y adjuntos viajan ilegibles para terceros.
- El asunto o metadatos pueden permanecer visibles.

Firmar + Cifrar = remitente verificable + contenido protegido.



S/MIME APOYA CONTROLES TÉCNICOS, PERO NO REEMPLAZA EL CUMPLIMIENTO INTEGRAL

Debe implementarse junto a políticas, procesos, registros, gestión de riesgos e incidentes.

LEY 21.719 | PROTECCIÓN DE DATOS PERSONALES

- Vigencia plena: 1 de diciembre de 2026.
- Principios de confidencialidad y seguridad.
- Controles adecuados para preservar secreto y reducir acceso no autorizado.
- El cifrado puede ser una medida técnica relevante según riesgo.

LEY 21.663 | MARCO DE CIBERSEGURIDAD

- Prevención, contención, resolución y respuesta a incidentes.
- Protección de confidencialidad, integridad, disponibilidad y resiliencia.
- Enfoque en servicios esenciales y operadores de importancia vital.
- S/MIME protege un canal crítico: correo corporativo.

La evidencia de control importa: alcance, certificados emitidos, renovaciones, revocaciones, políticas y responsables.



GLOBALSIGN: ADMINISTRACIÓN CENTRALIZADA DE CERTIFICADOS S/MIME

El desafío no es sólo emitir certificados: es gobernar el ciclo de vida completo.

DEFINIR ALCANCE

- Áreas sensibles, usuarios, casillas y dispositivos.

DESPLEGAR

- Emisión de certificados y distribución por políticas.

AUTOMATIZAR

- MPKI/CAM, Active Directory, Entra ID o MDM.

GOBERNAR

- Renovación, revocación, auditoría y reportes.

VMC: CERTIFICADO DE MARCA VERIFICADA

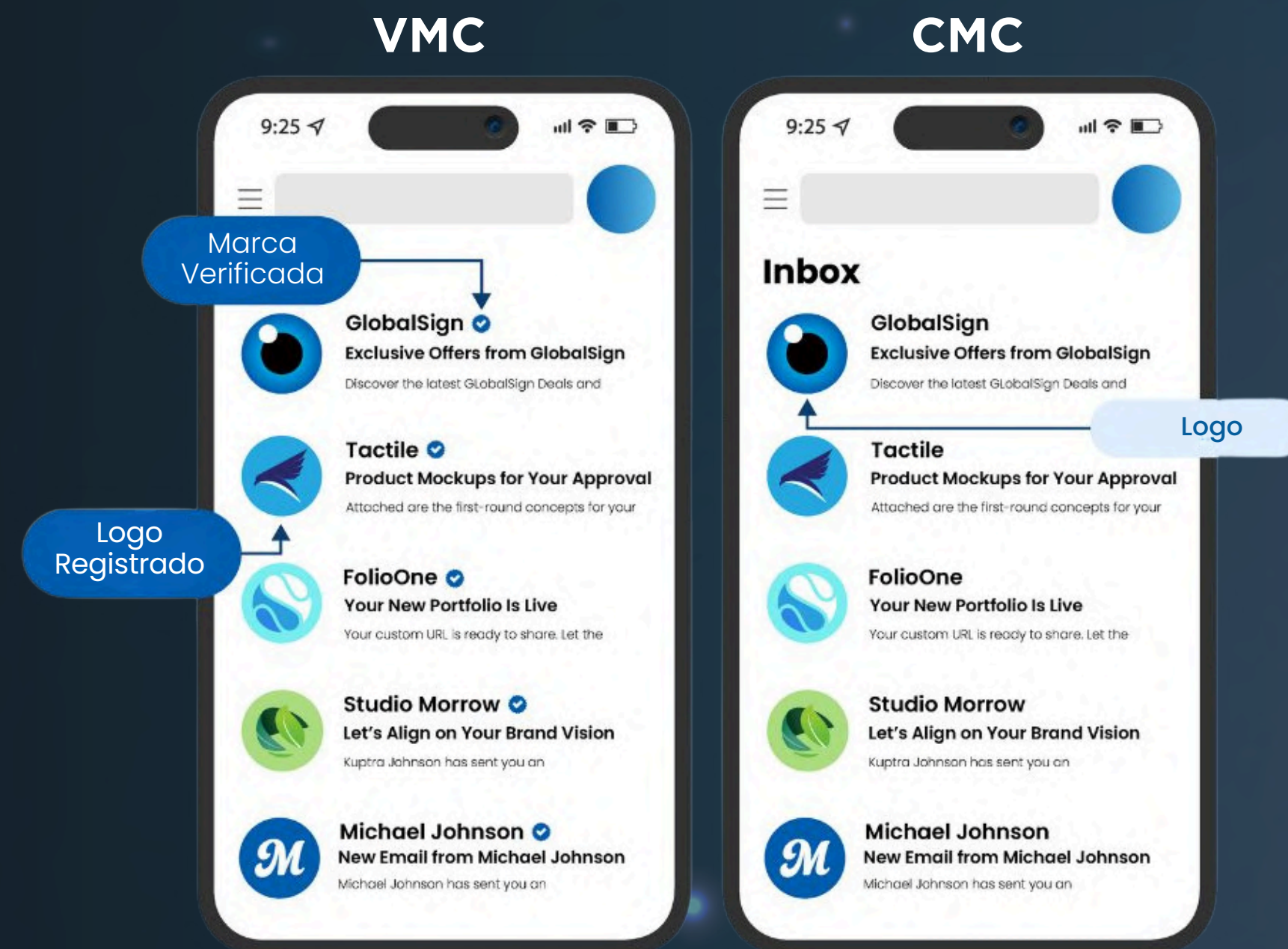
Para marcas registradas que buscan el mayor nivel de validación visual en correo, reforzando confianza y protección ante suplantación.

CMC: CERTIFICADOS DE MARCA COMÚN

Permiten a las empresas colocar el logotipo de una marca junto al campo "remitente" en las bandejas de entrada de los clientes, incluso antes de abrir el mensaje.

El logotipo actúa como confirmación del estado DMARC (Autenticación, informes y conformidad de mensajes basados en dominio) de su dominio y de la identidad autenticada de su organización.

Los CMC también brindan validación y seguridad adicionales para ayudar a proteger a sus clientes y su marca contra ataques de phishing y su plantación de identidad.





13 años

www.seguridadamerica.com

WEBINAR EDUCATIVO GLOBALSIGN

Gracias por Participar!

Diego López | Seguridad América
Antonio Gutiérrez | GlobalSign

