

INFORME · OCTUBRE 2026 · MES DE LA CIBERSEGURIDAD

CIBERCRIMEN 2026: LA IDENTIDAD DEL CORREO EN JUEGO

Suplantación con IA, dominios similares, interceptación y nuevas leyes de datos. Qué está pasando, cómo están Chile, Perú y Argentina, y cómo pasar de **p=none a la protección real**.

~90%

de 1,65 millones de dominios analizados sigue expuesto a suplantación

+USD 3.000 M

en pérdidas por compromiso de correo corporativo (BEC) en 2025

9,9%

de los dominios chilenos analizados aplicaba DMARC en p=reject

CONTENIDO

- 01 Hallazgos clave
- 02 El panorama de amenazas 2026
- 03 Latinoamérica: Chile, Perú y Argentina
- 04 El estado de DMARC en 2026
- 05 Fundamentos: SPF, DKIM, DMARC y lo que viene
- 06 Mitos y realidades sobre DMARC
- 07 Suplantación y dominios similares
- 08 MITM y cifrado en tránsito
- 09 BIMl y certificados de marca
- 10 Certificados SSL/TLS: de 398 a 47 días
- 11 Marco normativo y mandatos
- 12 El costo para el negocio
- 13 Plan de acción: de p=none a la protección
- 14 Diagnóstico gratuito y fuentes

INTRODUCCIÓN

DMARC pasó de buena práctica a requisito: Google, Yahoo y Microsoft lo exigen a los remitentes masivos y los reguladores avanzan en la misma dirección. Pero **publicar un registro no es lo mismo que estar protegido**. La IA generativa abarató el costo de suplantar una identidad, y la distancia entre “tenemos DMARC” y “bloqueamos la suplantación” es hoy la razón por la que los atacantes tienen éxito.

Este informe reúne datos recientes de la industria, la situación de Chile, Perú y Argentina, y un plan concreto para cerrar esa brecha.

01 · HALLAZGOS CLAVE

Lo más importante de este informe en una página.

Amenazas a la identidad del correo

USD 4,99 M

costo promedio global récord de una filtración de datos en 2026

+56%

alza interanual de los ataques con IA; cuestan ~USD 1 M más que el promedio

#1

phishing y spoofing: el delito más denunciado al FBI en 2025

El estado de DMARC

10,3%

de los dominios analizados llegó a la aplicación plena con p=reject

54%

de una cohorte de dominios siguió en p=none tres años seguidos

55,3%

de los dominios que empezaron en p=none en 2024 seguía ahí en 2026

Latinoamérica

63,8%

de los dominios chilenos analizados no tenía registro DMARC

74%

de las brechas en América Latina y el Caribe involucra a terceros

~0–1,2%

adopción de MTA-STS en Chile, Perú y Argentina

Fuente: IBM Cost of a Data Breach 2026; FBI Internet Crime Report 2025; PowerDMARC, informes de adopción por país (2024); Verizon DBIR 2026.

02 · EL PANORAMA DE AMENAZAS 2026

Lo que llega a la bandeja de entrada no se ve muy distinto que hace un año. **Lo que cambió es lo que hay detrás.** La IA puso capacidad de ataque avanzada al alcance de cualquiera: la barrera de entrada no solo bajó, prácticamente desapareció.

191.561

denuncias de phishing y spoofing al FBI en 2025

+USD 3.000 M

en pérdidas por BEC, con 8 veces menos denuncias

USD 893 M

en pérdidas por 22.364 denuncias de fraude con IA

Fuente: FBI Internet Crime Report 2025.

Menos correos, mejor dirigidos

Los atacantes no necesitan enviar más correos para ganar más. Una sola suplantación bien armada, enviada a la persona indicada con el pretexto indicado, rinde más que el spam masivo. El impacto además crece con el tamaño de la víctima:

USD 38.000

impacto mediano por incidente en pymes

USD 96.000

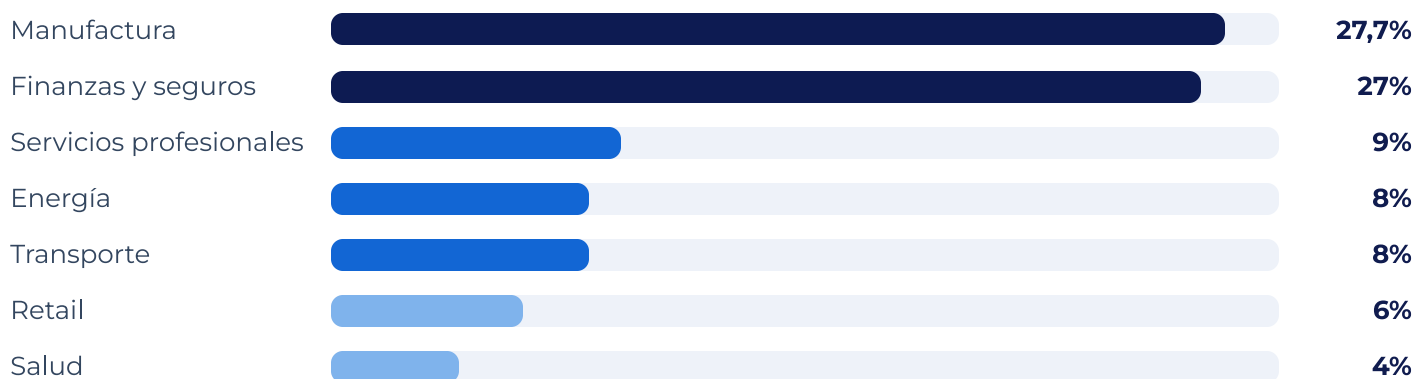
en empresas medianas (~150% más)

USD 283.000

en grandes empresas (más de 7 veces)

Fuente: Verizon Breach Impact Study 2026.

Industrias más atacadas en 2025



Fuente: Statista, distribución global de ciberataques por industria 2025.

El fraude de proveedores domina el BEC

El compromiso de correo de proveedores (VEC) ya representa cerca del **61% de la actividad BEC**. Las casillas compartidas como facturas@ o compras@ son especialmente vulnerables: nadie es dueño de ellas, y una factura falsa se mezcla en una fila llena de facturas

legítimas. El fraude de proveedores concentra el **81%** de los ataques BEC que llegan a una casilla compartida.

Caritas Luxemburgo · 2024

Perdió cerca de **USD 67 millones** por un fraude del falso presidente: un delincuente que suplantaba a un directivo logró más de 8.200 transferencias fuera del proceso de autorización.

Dickinson Public Schools · febrero 2026

Delincuentes que suplantaban a un proveedor desviaron dos pagos por **USD 4,92 millones**. El FBI logró rastrearlos y recuperarlos casi por completo.

La IA cambia quién ataca, no solo cómo

Los kits de **phishing como servicio (PhaaS)** generan un enlace y un adjunto únicos en cada envío y derrotan las listas de bloqueo. La plataforma **VENOM** evadió la detección al menos nueve meses, interceptando inicios de sesión de Microsoft y códigos MFA en tiempo real; el 60% de sus objetivos fueron ejecutivos y directores.

Un dato incómodo: los atacantes también **configuran DMARC, incluso en p=reject, en sus propios dominios falsos** para parecer más creíbles. Por eso DMARC protege su dominio, pero no reemplaza la vigilancia de dominios similares.

“La IA habilita el spear phishing a escala: un criminal que apunta a una empresa de 10.000 empleados puede atacarlos a todos con 10.000 correos únicos.”

Mike Britton, CIO

El Global Cybersecurity Outlook 2026 del Foro Económico Mundial halló que el **fraude y el phishing** pasaron a ser la principal preocupación de los CEO, superando por primera vez al ransomware.

03 · LATINOAMÉRICA: CHILE, PERÚ Y ARGENTINA

El Data Breach Investigations Report 2026 de Verizon halló que el **74% de las brechas** en América Latina y el Caribe involucra a terceros, la tasa más alta entre las regiones medidas. El phishing es el segundo vector de acceso inicial (20%) y hay motivo financiero en el 90% de los casos. A eso se suma una brecha de capacidades: el **69% de los CEO** de la región dice no tener las habilidades para cumplir sus objetivos de ciberseguridad.

Comparativa de adopción de autenticación por país

Indicador	Chile	Perú	Argentina
SPF configurado	70,0%	86,1%	95,2%
DMARC en p=reject	9,9%	17,9%	18,5%
Sin registro DMARC	63,8%	33,0%	—
Sin protección efectiva	~90%	82% en monitoreo	56,9%
MTA-STS	~0%	0,6%	1,2%

Fuente: PowerDMARC, informes de adopción de DMARC por país (análisis de ~1.000 dominios por país, 2024). Datos anteriores a 2026; se incluyen como referencia de la brecha regional.

Chile · el país con menor adopción de la región

Sobre 1.004 dominios analizados, el **63,8% no tenía registro DMARC** y solo el 9,9% aplicaba p=reject. Los sectores más expuestos fueron **energía (77,4% sin DMARC)** y medios (74,6%). La adopción de MTA-STS era prácticamente nula. Chile registró 9.400 millones de intentos de ciberataque en 2021.

Perú · la “trampa del monitoreo”

El 86,1% de los dominios tiene SPF, pero **más del 82% de quienes usan DMARC sigue en p=none**: ven el problema, pero no lo bloquean. Telecomunicaciones es el sector más vulnerable (43,3% sin DMARC). La Ley 29733, reforzada por el DS 016-2024-JUS, exige controles alineados con ISO 27001 y notificar brechas en **48 horas**.

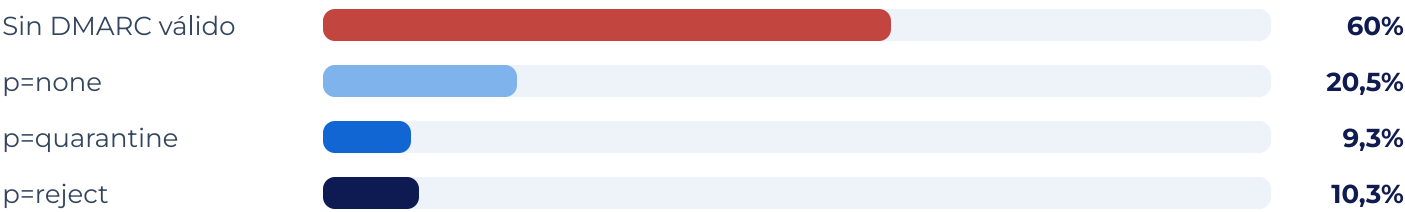
Argentina · base técnica sólida, poca aplicación

Con 95,2% de SPF correcto, solo el 18,5% aplica p=reject y el **56,9% de los dominios sigue sin protección efectiva**. Los ataques de phishing crecieron 44% interanual y el gobierno concentró el 61% de los 438 incidentes que gestionó CERT.ar en 2024. La Ley 25.326 exige medidas de seguridad técnicas adecuadas.

04 · EL ESTADO DE DMARC EN 2026

Un análisis de la industria sobre 1,65 millones de dominios, realizado entre febrero de 2024 y junio de 2026, concluye que **la adopción sube, pero la aplicación no la acompaña**.

Distribución de políticas DMARC



Casi el 90% de los dominios está expuesto: sin DMARC, o con una política que no bloquea nada. **p=reject es la única política que detiene la suplantación antes de que llegue a la bandeja.**

Adopción vs. aplicación (cohorte de 34.212 dominios)

Corte	DMARC válido	p=reject	Brecha
Junio 2024	48,6%	12,6%	36 pts
Junio 2025	63,1%	19,7%	43,4 pts
Junio 2026	71,5%	26,6%	44,9 pts

La brecha entre tener DMARC y aplicarlo **se amplió** en dos años. De los dominios que empezaron en p=none en 2024, el 55,3% seguía ahí en 2026 y apenas uno de cada cinco (20,7%) llegó a p=reject.

“Un registro de solo monitoreo no protege al dueño del dominio: le avisa al mundo que se espera que su correo falle la evaluación DMARC.”

Kieran Frost, COO

Gestionado vs. autogestionado

Llegar a p=none es fácil; lo difícil es terminar el camino. Las implementaciones acompañadas completan el paso a p=reject con mucha más frecuencia que las autogestionadas, que tienden a estancarse en p=quarantine:

93,9%

tasa de finalización en
implementaciones
gestionadas

69,1%

con otros proveedores
DMARC

37,5%

en implementaciones
autogestionadas (DIY)

Fuente: análisis de la industria. Tasa de finalización = $p=\text{reject} \div (p=\text{reject} + p=\text{quarantine})$. Promedio para llegar a $p=\text{reject}$: 64,6 días en 1.207 proyectos gestionados.

La infraestructura se concentra: en los datos observados, **Microsoft y Google suman el 80,4%** de la categoría de proveedores de correo, frente al 56,9% en 2024.

05 · FUNDAMENTOS: SPF, DKIM, DMARC Y LO QUE VIENE

Los tres protocolos trabajan juntos. Ninguno basta por sí solo.

SPF · RFC 7208

Declara en el DNS qué servidores pueden enviar correo por su dominio. Límite de **10 consultas DNS**: superarlo invalida el registro, un error común cuando se suman proveedores en la nube.

DKIM · RFC 6376

Firma cada mensaje con una clave criptográfica y prueba que el contenido no fue alterado. Se recomiendan claves RSA de **2048 bits** y rotación periódica.

DMARC · RFC 7489 / RFC 9989

Une SPF y DKIM con el dominio visible del remitente (**alineación**), indica qué hacer con lo que falla y envía **reportes** de quién envía en su nombre. DMARCBis (RFC 9989) actualiza el estándar.

El camino a p=reject

p=none

Solo monitorea. **No protege**, pero entrega visibilidad.

p=quarantine

Lo que falla va a spam. Protección parcial.

p=reject

Lo que falla se rechaza. **Suplantación bloqueada.**

Subdominios: el punto ciego

La política del dominio principal la heredan los subdominios sin registro propio. Muchas organizaciones ni saben qué subdominios envían correo: los reportes DMARC son la mejor forma de descubrir toda la huella.

DKIM2: lo que viene

El DKIM original permite que un correo legítimo y firmado se **reenvíe a destinatarios no previstos** y siga pasando la verificación, incluso con p=reject. El IETF trabaja en **DKIM2** para resolverlo. Google y Yahoo planean pruebas experimentales en el último trimestre de 2026 y despliegue productivo en 2027. Los registros DKIM actuales siguen válidos.

“Hacen falta los reportes para descubrir dónde están los huecos de autenticación, corregirlos y recién ahí pasar a quarantine o reject.”

Todd Herr, coeditor del RFC 9989 · IETF, RFC 9989

06 · MITOS Y REALIDADES

Ideas comunes que frenan la protección del correo:

01 “DMARC es un filtro de spam.”

No filtra el correo entrante. Protege su identidad saliente: le indica a los receptores qué hacer con los correos que dicen venir de su dominio.

02 “Se configura una vez y listo.”

Cada nuevo CRM o proveedor cambia el mapa de envío. Sin monitoreo, el registro que protegía el trimestre pasado puede no proteger hoy.

03 “Con publicarlo ya estoy protegido.”

La aplicación ocurre en el receptor y solo si la política es quarantine o reject. Con p=none no hay nada que aplicar.

04 “Garantiza que llegue a la bandeja.”

Ayuda a la entregabilidad, pero no reemplaza una buena reputación de envío.

05 “Los reportes son fáciles de leer.”

Llegan como XML crudo desde decenas de fuentes. Sin una plataforma, leerlos frena muchos proyectos.

06 “Mi correo pasa por el proveedor DMARC.”

No. DMARC funciona por DNS. El proveedor solo recibe metadatos de autenticación, nunca el contenido de los mensajes.

07 “Aplicar DMARC rompe mi correo.”

Bien hecho, mejora la entrega. El riesgo viene de apurar la aplicación antes de identificar a cada remitente.

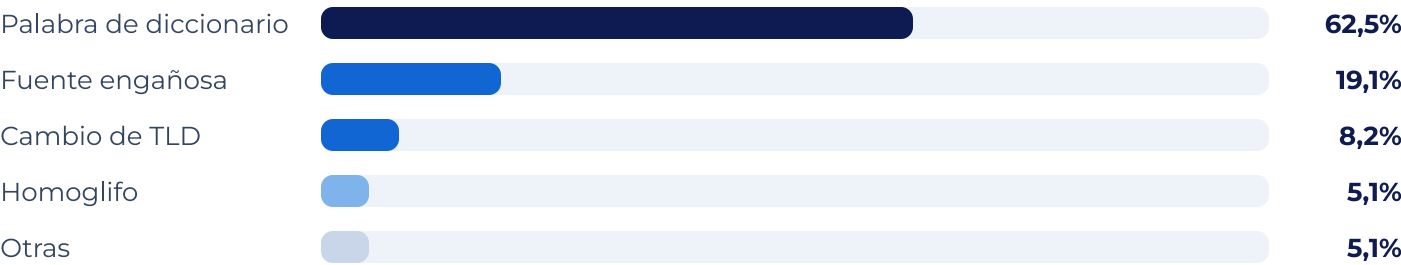
08 “Si tengo SPF y DKIM, no necesito DMARC.”

DMARC es la capa que los ata al remitente visible, los vuelve exigibles y entrega los reportes.

07 · SUPLANTACIÓN Y DOMINIOS SIMILARES

Técnica	Cómo funciona	Defensa
Spoofing de dominio exacto	Usa su dominio real en el remitente sin autorización.	DMARC en p=reject
Dominio similar (lookalike)	Registra un dominio casi igual: suempresa-soporte.com, banc0.cl.	Monitoreo de dominios y BIMI
Nombre visible falso	Muestra “Banco XYZ 🔒 ” desde una cuenta gratuita.	BIMI y capacitación
BEC / fraude del CEO	Se hace pasar por un ejecutivo o proveedor para pedir pagos.	DMARC y doble validación
Cuenta comprometida	Envía desde una casilla legítima robada: pasa la autenticación.	MFA y monitoreo de reportes

DMARC detiene el spoofing exacto, por eso los atacantes migran a dominios similares. Las técnicas más usadas entre 2023 y 2026:



Fuente: análisis de la industria, promedio global junio 2023–junio 2026.

Los **homoglifos** (una “a” cirílica en lugar de una “a” latina) casi se triplicaron y son casi imposibles de distinguir a simple vista. Además, los errores de tipeo y los subdominios reordenados, aunque son pocos, tienen muchas más probabilidades de tener un sitio o correo activo detrás: son los que se convierten en arma.

08 · MITM Y CIFRADO EN TRÁNSITO

Entre servidores, el correo se cifra con **STARTTLS** de forma oportunista: si un atacante intermedio elimina el anuncio de cifrado, el mensaje viaja **en texto plano** sin que nadie lo note. Es un ataque de degradación típico de un hombre en el medio (MITM).

MTA-STS · RFC 8461

Obliga a los servidores remitentes a usar TLS con un **certificado válido** al entregar correo a su dominio. Sin TLS, no hay entrega.

TLS-RPT · RFC 8460

Envía reportes diarios de fallos de cifrado: permite detectar intentos de interceptación y errores de configuración.

DANE · RFC 7672

Alternativa basada en DNSSEC que fija el certificado esperado directamente en el DNS.

~0%

adopción de MTA-STS en Chile

0,6%

en Perú

1,2%

en Argentina

Fuente: PowerDMARC, informes de adopción por país (2024).

En la región, casi todo el correo que viaja entre servidores **puede ser interceptado o degradado**, incluso cuando está autenticado. MTA-STS depende además de un certificado SSL/TLS válido: si vence, la protección se cae.

09 · BIMI Y CERTIFICADOS DE MARCA

SPF, DKIM y DMARC trabajan donde el usuario no mira. **BIMI** traduce ese resultado a algo visible: el **logo oficial de la marca** junto al remitente, imposible de copiar por un atacante.

- Requiere DMARC en **p=quarantine o p=reject**: es un incentivo directo para llegar a la aplicación.
- El logo debe publicarse en formato **SVG Tiny PS**.
- Se respalda con un certificado de marca de DigiCert: **VMC** (marca registrada en una oficina reconocida) o **CMC** (sin registro de marca, la opción viable para gran parte de Latinoamérica).
- Cada proveedor de correo define sus propios criterios para mostrar el logo.

Por qué importa ahora

Si los atacantes ya configuran DMARC en sus dominios falsos, la autenticación por sí sola deja de ser una señal visible de confianza. El logo verificado sí lo es.

10 · CERTIFICADOS SSL/TLS: DE 398 A 47 DÍAS

El CA/Browser Forum aprobó reducir de forma escalonada la vigencia máxima de los certificados públicos:

Desde	Vigencia máxima	Renovaciones al año
Hasta marzo 2026	398 días	~1
15 marzo 2026	200 días	~2
15 marzo 2027	100 días	~4
15 marzo 2029	47 días	~8

Fuente: CA/Browser Forum, Ballot SC-081.

Con cientos de certificados, renovar a mano multiplica el riesgo de caídas por vencimiento, y un certificado vencido también tumba MTA-STTS. **DigiCert Trust Lifecycle Manager (TLM)** descubre, emite, instala y renueva certificados de forma automática, con inventario centralizado y sin abrir puertos de entrada en su red.

El candado no es identidad

Un certificado DV se obtiene gratis en minutos y los sitios de phishing lo usan. Los certificados **OV y EV** verifican la existencia legal de la empresa.

11 · MARCO NORMATIVO Y MANDATOS

Proveedores de correo

Fecha	Mandato
Feb 2024	Google y Yahoo exigen SPF, DKIM y DMARC (p=none mínimo) a remitentes de más de 5.000 correos diarios.
Mar 2025	PCI DSS v4.0.1 exige mecanismos antiphishing a quienes procesan pagos con tarjeta.
May 2025	Microsoft exige DMARC a remitentes masivos en Outlook.
Nov 2025	Google pasa a rechazos temporales y permanentes del correo que no cumple.
May 2026	GMX, WEB.DE y mail.com anuncian mandato DMARC con despliegue gradual a p=reject.

Ninguno de los grandes proveedores exige todavía p=reject: **se puede cumplir con todos sin bloquear nada**. Es una de las razones de la brecha entre adopción y aplicación.

Chile

Ley 21.663 · Ley Marco de Ciberseguridad

Vigente desde marzo de 2025. Crea la **ANCI**, exige controles de seguridad a operadores de importancia vital y notificar incidentes al CSIRT Nacional en plazos acotados.

Ley 21.719 · Protección de Datos Personales

Entra en vigencia el **1 de diciembre de 2026**. Crea la Agencia de Protección de Datos Personales, impone deber de seguridad, notificación de brechas y multas de hasta **20.000 UTM** por infracciones gravísimas.

Perú y Argentina

Perú • Ley 29733 y DS 016-2024-JUS

Controles alineados con ISO 27001 y notificación de brechas en **48 horas**, bajo la supervisión de la ANPDP.

Argentina • Ley 25.326

Exige medidas técnicas y organizativas adecuadas para proteger los datos personales, bajo la AAIP. CERT.ar recomienda la autenticación del correo.

Ninguna de estas leyes nombra DMARC, pero todas exigen **medidas de seguridad adecuadas y demostrables**. Un correo suplantado que filtra datos de clientes puede originar una brecha notificable. Recomendamos validar el alcance con su asesor legal.

12 · EL COSTO PARA EL NEGOCIO

Un dominio en p=None no puede impedir que un correo fraudulento llegue a la bandeja. El riesgo no es solo técnico:

1

Daño financiero

Contener el ataque es solo el inicio: vienen abogados, multas, primas más altas y clientes que se van.

2

Confianza erosionada

Un dominio suplantado puede deshacer en días años de reputación. El 41% del ransomware ya incluye amenazas a la reputación de la marca.

3

Comunicación rota

Un dominio en listas de bloqueo corta el contacto con clientes, proveedores y socios.

4

Operación detenida

Un pago fraudulento, una conversación secuestrada o un ransomware paralizan los procesos.

5

Exposición normativa

Correo rechazado, sanciones o la suspensión de la capacidad de procesar pagos.

USD 4,99 M

costo promedio global de una filtración (IBM 2026)

USD 1.100

costo por hora de una filtración

USD 11,5 M

costo promedio en EE. UU., el doble del global

Prevenir la suplantación cuesta mucho menos que recuperarse de ella.

13 · PLAN DE ACCIÓN: DE P=NONE A LA PROTECCIÓN

Ninguna acción aislada lleva de expuesto a protegido. Es una secuencia, y saltar pasos es lo que rompe el correo legítimo en el camino.

- 1 **Inventariar.** Todos los servicios que envían correo con su dominio: CRM, facturación electrónica, marketing, RR. HH.
- 2 **Bases bien puestas.** SPF sin superar 10 consultas DNS y DKIM de 2048 bits en cada plataforma.
- 3 **Publicar p=none con reportes.** Activar la etiqueta rua y leer los reportes con una plataforma, no en XML crudo.
- 4 **Corregir y autorizar.** Alinear cada remitente legítimo, incluidos los subdominios.
- 5 **p=quarantine.** Enviar lo sospechoso a spam mientras se vigilan los reportes.
- 6 **p=reject.** Rechazar lo no autenticado. El dominio ya no puede usarse para suplantar.
- 7 **Dominios sin correo.** Proteger con p=reject los dominios que no envían correo.
- 8 **MTA-STS y TLS-RPT.** Forzar el cifrado en tránsito y monitorear sus fallos.
- 9 **BIMI.** Publicar el logo con certificado VMC o CMC.
- 10 **Vigilar y automatizar.** Monitorear dominios similares y automatizar los certificados SSL/TLS antes de los 100 días.

“Si configuró y aplicó DMARC correctamente, un atacante no puede autenticarse como su dominio, por convincente que sea el mensaje.”

Keith Thompson, CTO

Cómo lo hacemos en Digitalcorp LATAM

Implementamos **PowerDMARC** para la visibilidad y el camino guiado a p=reject, con MTA-STS, TLS-RPT y BIMI alojados; certificados **VMC/CMC** de DigiCert, y **DigiCert Trust Lifecycle Manager** para automatizar los certificados SSL/TLS. Con soporte local en español.

14 · DIAGNÓSTICO GRATUITO

REVISE SU DOMINIO HOY EN **TOOLS.DIGITALCORPLATAM.COM**

Herramientas sin costo y sin instalar nada. En minutos sabe en qué punto del plan de acción está su dominio.

Analizador DMARC · SPF, DKIM, DMARC, MTA-STS, TLS-RPT y BIMI de su dominio

Analizador SPF · conteo de consultas DNS (límite RFC 7208)

Formateador BIMI · logo a SVG Tiny PS

Verificador SSL · validez, cadena y vencimiento

Cabeceras HTTP · HSTS, CSP y más

Analizador de encabezados · ruta de entrega y resultado de autenticación

Consulta DKIM · clave, longitud y tipo

MTA-STS · TLS-RPT · política de cifrado en tránsito

Decodificador CSR · dominio, SAN y algoritmo

tools.digitalcorplatam.com

Referencia de estándares

Estándar	Documento	Protege
SPF	RFC 7208	Servidores autorizados
DKIM	RFC 6376 · DKIM2 en desarrollo	Integridad del mensaje
DMARC	RFC 7489 · RFC 9989 (DMARCBis)	Alineación, política y reportes
ARC	RFC 8617	Autenticación en reenvíos
MTA-STS	RFC 8461	Cifrado obligatorio en tránsito
TLS-RPT	RFC 8460	Reportes de fallos de cifrado
DANE	RFC 7672	Certificado fijado vía DNSSEC
BIMI	BIMI Group	Logo verificado de la marca

Fuentes: IETF — RFC 7208 (SPF), RFC 6376 (DKIM), RFC 7489 y RFC 9989 (DMARC / DMARCBis), RFC 8617 (ARC), RFC 8461 (MTA-STS), RFC 8460 (TLS-RPT), RFC 7672 (DANE), RFC 5321 (SMTP) y RFC 3207 (STARTTLS); PowerDMARC, informes de adopción de DMARC en Chile, Perú y Argentina (2024); FBI IC3 Internet Crime Report 2025; IBM Cost of a Data Breach Report 2026; Verizon DBIR 2026 y Breach Impact Study 2026; WEF Global Cybersecurity Outlook 2026; Statista; CA/Browser Forum Ballot SC-081; BIMI Group; Biblioteca del Congreso Nacional de Chile. Cada cifra debe leerse en el contexto de su fuente. Digitalcorp LATAM es partner de DigiCert y PowerDMARC en Latinoamérica. Este informe es informativo y no constituye asesoría legal.