

Suplantación de correo en el IBEX 35

Una de cada cuatro empresas del índice no bloquea el correo que suplanta su dominio. Análisis de DMARC, SPF, MTA-STS y cabeceras de seguridad web de las 35 compañías.

9 de 35

sin política DMARC que bloquee o aparte el correo falso

6 de 8

en p=none reciben informes que lo muestran y no bloquean

63 %

aplican la política más estricta, p=reject



Estudio dirigido por **Thilina Manana**
Director de Operaciones y Seguridad
Octubre de 2026

01	Resumen ejecutivo y principales hallazgos	2
02	Resultados: política DMARC y comparación con la gran empresa	3
03	Otras protecciones, portada web y recomendaciones	4
04	Metodología, datos abiertos y contacto de prensa	5

Nueve empresas del IBEX 35 dejan abierta la suplantación de su dominio de correo

En septiembre de 2026, 9 de las 35 empresas del IBEX 35 (26 %) no tienen una política DMARC que bloquee o aparte el correo que suplanta su dominio: 8 están en p=none y 1 no publica registro. El 63 % aplica la política más estricta, p=reject, 25 puntos más que la gran empresa española en su conjunto (38 %).

9/35

no bloquean ni apartan el correo que suplanta su dominio

6/8

en p=none reciben informes DMARC y siguen sin bloquear

63 %

en p=reject, frente al 38 % de 219 grandes empresas

1/35

obliga a cifrar el correo que recibe (MTA-STS)

Principales hallazgos

- **La cola sin proteger es igual de larga que en el resto de la gran empresa.** El IBEX aplica p=reject mucho más (63 % frente a 38 %), pero la proporción sin una política que bloquee es prácticamente la misma (26 % frente a 27 %).
- **Ven la suplantación y no la bloquean.** 6 de las 8 empresas en p=none reciben a diario informes con los servidores que envían en su nombre, incluidos los no autorizados.
- **SPF está generalizado; el cifrado en la entrega, no.** Las 35 publican SPF, pero solo 1 publica MTA-STS, 2 TLS-RPT y 4 BIMi.
- **La mitad de las portadas web no tiene Content-Security-Policy** (15 de 30 con respuesta válida) y 4 no tienen HSTS.
- **El problema tiene solución conocida.** Pasar a p=reject sin perder correo legítimo es un proceso ordenado de entre uno y tres meses en una organización grande.

RESULTADOS

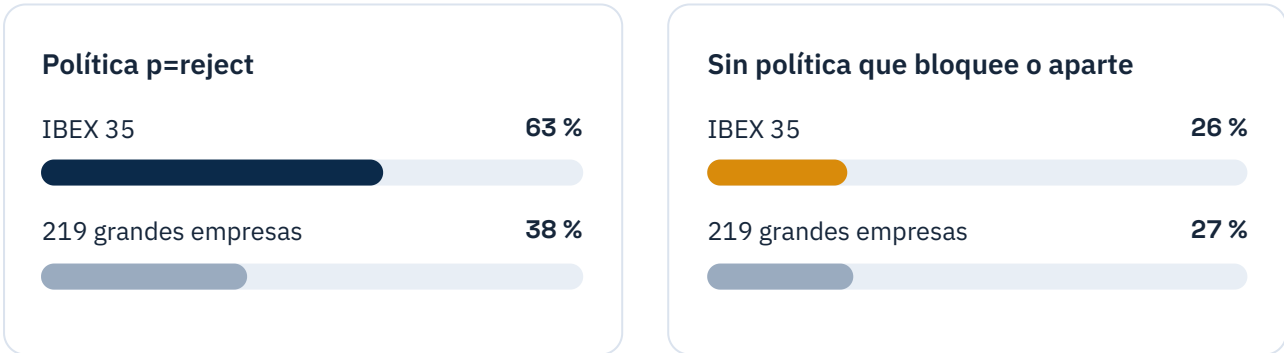
Qué política DMARC aplican las empresas del IBEX 35

DMARC es el registro con el que el propietario de un dominio indica qué hacer con los correos que dicen venir de él y no superan las comprobaciones SPF y DKIM. Es la defensa directa contra el correo falso que usa exactamente el dominio de la empresa, base de muchos fraudes del CEO y de cambio de cuenta bancaria.



POLÍTICA	QUÉ HACE EL RECEPTOR CON EL CORREO FALSO	EMPRESAS	%
 p=reject	Lo rechaza.	22	62,9
 p=quarantine	Lo aparta, normalmente a spam.	4	11,4
 p=none	Lo entrega con normalidad; solo se generan informes.	8	22,9
 Sin registro	No hay política publicada.	1	2,9

Comparación con 219 grandes empresas españolas



Fuente de la comparación: Radiografía DMARC de las grandes empresas españolas, Hard2bit, 7 de septiembre de 2026.

6 de 8

empresas en p=none publican una dirección para recibir informes agregados (rua). Cada día reciben el detalle de los servidores que envían correo en su nombre, incluidos los no autorizados, y aun así no piden a los receptores que los bloqueen. Lo habitual es un despliegue que se quedó a medias por miedo a perder correo legítimo.

OTRAS PROTECCIONES DEL CORREO

CONTROL	EMPRESAS
SPF publicado (30 con -all, 5 con ~all)	35/35
SPF con 9 o 10 consultas DNS (límite 10)	4/35
BIMI (logotipo verificado)	4/35
TLS-RPT (informes de cifrado)	2/35
MTA-STS (cifrado obligatorio)	1/35

DKIM no se incluye: sus claves se publican bajo selectores que cada empresa elige y no pueden enumerarse desde fuera.

LA PORTADA WEB

CABECERA AUSENTE	PORTADAS
Content-Security-Policy	15/30
HSTS	4/30
Protección contra clickjacking	3/30

30 de 35 portadas devolvieron la página; 5 respondieron con un bloqueo del cortafuegos o un desafío anti-bot y se excluyen.

RECOMENDACIONES

Cómo llegar a p=reject sin perder correo legítimo

01

Inventariar quién envía en tu nombre

Correo corporativo, CRM, facturación, nóminas, marketing y avisos automáticos. Los informes DMARC muestran los que faltan.

03

Pasar a quarantine de forma gradual

Con el parámetro pct, por tramos, mientras se revisan los informes.

05

Cubrir los dominios secundarios

Los que no envían correo necesitan SPF -all y DMARC p=reject igualmente.

02

Firmar con DKIM todos los envíos legítimos

Cada plataforma con su selector: es lo que mantiene el correo legítimo cuando la política se endurece.

04

Llegar a p=reject

Incluidas las políticas de subdominios (sp) y de subdominios inexistentes (np).

06

Proteger el transporte

MTA-STS y TLS-RPT para exigir cifrado en la entrega y saber cuándo falla.

Cómo se ha hecho el estudio

Análisis pasivo con información pública, el mismo que puede hacer cualquier persona. No se ha enviado correo a ninguna empresa ni se ha probado ninguna vulnerabilidad.

Muestra	Las 35 empresas del IBEX 35 según la composición publicada el 28 de septiembre de 2026.
Fecha	28 de septiembre de 2026. Los registros DNS cambian: el estudio es una fotografía de ese día.
Dominio analizado	El dominio de correo principal de cada empresa. Los dominios secundarios de 7 empresas se revisaron, pero no cuentan en los porcentajes (1 en p=none y 1 sin registro DMARC).
Correo	Consultas DNS de MX, SPF (con recuento de consultas anidadas), DMARC, MTA-STS, TLS-RPT, BIMI y selectores DKIM habituales.
Web	Una petición HTTPS a la portada, siguiendo redirecciones: HSTS, Content-Security-Policy, X-Frame-Options y frame-ancestors.
Anonimato	Resultados agregados. No se identifica a ninguna empresa.

DATOS ABIERTOS Y CITA

Los indicadores agregados se publican con licencia Creative Commons Reconocimiento 4.0 en hard2bit.com/estudios/suplantacion-correo-ibex-35/, con descarga en CSV.

Manana, T. (2026). Suplantación de correo en el IBEX 35. Hard2bit. Datos del 28 de septiembre de 2026.
<https://hard2bit.com/estudios/suplantacion-correo-ibex-35/>

SOBRE HARD2BIT

Empresa española de ciberseguridad fundada en 2013, con sede en el Parque Tecnológico de Leganés (Madrid). Certificada en el Esquema Nacional de Seguridad, categoría ALTA, y en ISO/IEC 27001, ISO 22301, ISO/IEC 20000-1, ISO 9001 e ISO 14001.



Prensa y analistas

Para datos adicionales o una entrevista con el equipo: info@hard2bit.com · 910 139 827 · hard2bit.com/prensa