HERMES SECURITY

Guía de Remediación Técnica



Dominio:	test-domain-12345.com
Fecha:	17 de noviembre de 2026
Tipo:	Guía de corrección de vulnerabilidades
Clasificación:	CONFIDENCIAL - Solo para el destinatario

Hermes Security | cyberdefense.valencia@proton.me | cybersofia.tech

Resumen Ejecutivo

El análisis de seguridad de **test-domain-12345.com** ha obtenido una puntuación global de **62/100**, con un nivel de riesgo **MEDIO**. Se han detectado **17 problemas** que requieren atención.

Principales riesgos detectados:

1. Conexiones cifradas inestables o certificado con problemas

Recomendación: abordar primero los hallazgos de severidad crítica y alta (correo, cabeceras, SSL y tecnologías con CVE), ya que son la puerta de entrada para un atacante. La guía detallada a continuación proporciona los pasos exactos para cada corrección.

Introducción

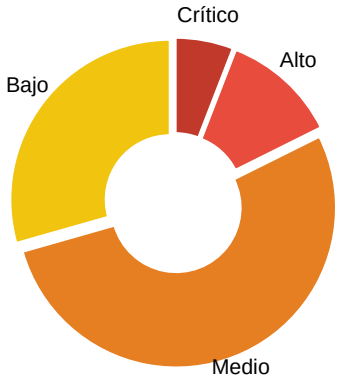
Este documento describe los pasos necesarios para corregir las vulnerabilidades y problemas de configuración detectados durante el análisis de seguridad. Las acciones están organizadas por prioridad y tipo de problema, con instrucciones claras pensadas para que puedan ser ejecutadas por personal técnico no especializado en seguridad.

Resumen de Hallazgos

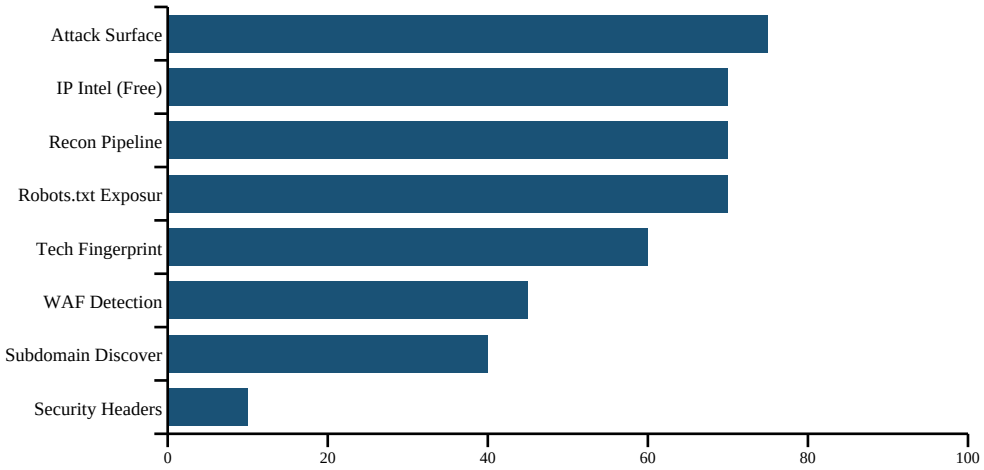
Métrica	Valor
Score Global	62/100
Problemas detectados	17
Nivel de riesgo	MEDIO
Dominio	test-domain-12345.com

Panorama Visual

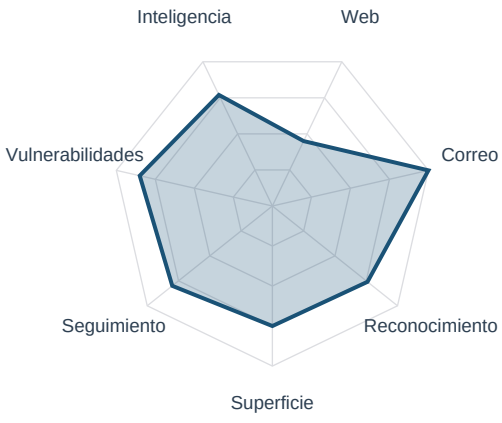
Distribución de hallazgos por severidad, score por módulo y salud por sector. Los módulos con score más bajo son los que requieren atención prioritaria.



Score por Módulo



Salud por Sector



Evidencia del Objetivo

Captura real del estado actual del objetivo. Esta evidencia permite verificar visualmente la configuración detectada y confirmar la remediación tras aplicar los cambios.



Headers HTTP devueltos por el servidor/CDN (evidencia de configuración).

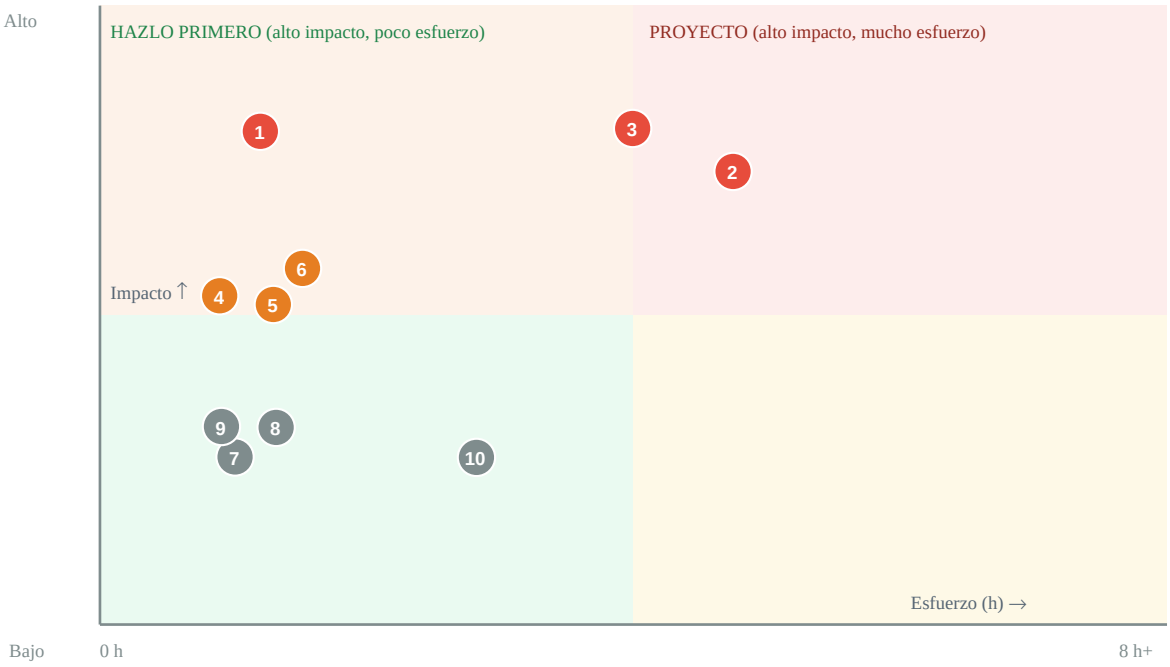
Plan de corrección por hallazgo

Se han identificado **10** problemas que requieren acción (3 alta, 3 media, 4 baja). Cada ficha incluye qué se midió, por qué importa, el cambio exacto por plataforma, cómo verificarlo y cuánto cuesta aplicarlo.

#	Prior.	Hallazgo	Esfuerzo	Responsable	Hecho
1	Alta	Falta la cabecera Strict-Transport-Security	15 min	Infraestructura	[ ]
2	Alta	Falta la cabecera Content-Security-Policy	2-4 h	Desarrollo + Infraestructura	[ ]
3	Alta	Subdominios sensibles expuestos	2 h	Desarrollo	[ ]
4	Media	Falta la cabecera X-Frame-Options	10 min	Infraestructura	[ ]
5	Media	Falta la cabecera X-Content-Type-Options	10 min	Infraestructura	[ ]
6	Media	robots.txt revela rutas sensibles	20 min	Desarrollo	[ ]
7	Baja	Falta la cabecera Referrer-Policy	10 min	Infraestructura	[ ]
8	Baja	Falta la cabecera Permissions-Policy	10 min	Infraestructura	[ ]
9	Baja	Falta la cabecera Cross-Origin-Opener-Policy	10 min	Infraestructura	[ ]
10	Baja	HSTS no detectado	1 h	Desarrollo / Infraestructura	[ ]

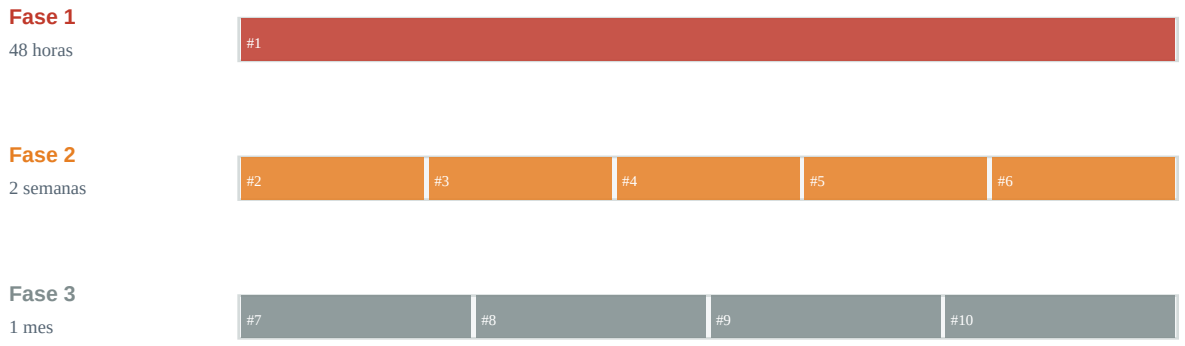
Qué abordar primero

Cada burbuja es una ficha y su número coincide con la tabla. Arriba a la izquierda está lo de alto impacto y poco esfuerzo: empieza por ahí.



Plan por fases

Reparto por urgencia: la fase 1 no espera a mañana, la 3 puede entrar en el ciclo normal de mantenimiento.



10 hallazgos repartidos por urgencia; las fases con más barras son las que piden más manos.

Ficha 1

Falta la cabecera Strict-Transport-Security

15 min · Infraestructura **[Alta]**

● **Qué riesgo implica:** Sin HSTS, el primer acceso por http:// puede ser interceptado (sslstrip): el atacante se queda con la sesión antes de la redirección.

Pasos para resolverlo:
1. Identifica dónde termina el TLS (CDN o servidor propio).
2. Añade la cabecera con el valor max-age=31536000; includeSubDomains.
3. Purga la caché del CDN y comprueba que la respuesta ya la incluye.

Cómo aplicarlo:

```
# Nginx
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains"
always;

# Apache
Header always set Strict-Transport-Security "max-age=31536000; includeSubDo
mains"

# Cloudflare (Rules > Transform Rules > Modify Response Header)
Set static  ·  Strict-Transport-Security: max-age=31536000; includeSubDomai
ns

# IIS (web.config)
<add name="Strict-Transport-Security" value="max-age=31536000; includeSubDo
mains" />
```

■ **Cuidado:** HSTS preload es irreversible. Prueba primero sin includeSubDomains.

■ **Verificar:** curl -sI https://test-domain-12345.com | grep -i 'strict-transport-security'

Ficha 2

Falta la cabecera Content-Security-Policy

2-4 h · Desarrollo + Infraestructura **[Alta]**

● **Qué riesgo implica:** Sin CSP cualquier XSS en la página se ejecuta con permisos plenos (robo de cookies, keylogging, redirección a phishing).

Pasos para resolverlo:
1. Identifica dónde termina el TLS (CDN o servidor propio).
2. Añade la cabecera con el valor default-src 'self'; object-src 'none'; base-uri 'self'; frame-ancestors 'self'.
3. Purga la caché del CDN y comprueba que la respuesta ya la incluye.

Cómo aplicarlo:

```
# Nginx
add_header Content-Security-Policy "default-src 'self'; object-src 'none';
base-uri 'self'; frame-ancestors 'self'" always;

# Apache
Header always set Content-Security-Policy "default-src 'self'; object-src '
none'; base-uri 'self'; frame-ancestors 'self'"

# Cloudflare (Rules > Transform Rules > Modify Response Header)
Set static  ·  Content-Security-Policy: default-src 'self'; object-src 'non
e'; base-uri 'self'; frame-ancestors 'self'

# IIS (web.config)
<add name="Content-Security-Policy" value="default-src 'self'; object-src '
none'; base-uri 'self'; frame-ancestors 'self'" />
```

■ **Cuidado:** Una CSP mal puesta rompe scripts inline. Implanta primero en Content-Security-Policy-Report-Only y revisa los informes.

■ **Verificar:** curl -sI https://test-domain-12345.com | grep -i 'content-security-policy'

Ficha 3

Subdominios sensibles expuestos

2 h · Desarrollo

[Alta]

● **Qué riesgo implica:** Entornos de desarrollo, staging o APIs internas accesibles desde internet suelen tener menos protección y datos reales.

Pasos para resolverlo:
1. Enumera los subdominios detectados y decide cuáles deben ser públicos.
2. Los de dev/staging: autenticación básica o VPN, nunca abiertos.
3. Revisa que no expongan datos de producción.

Cómo aplicarlo:

```
# Nginx: cerrar un vhost con autenticación básica
auth_basic "Staging";
auth_basic_user_file /etc/nginx/.htpasswd;
```

■ **Verificar:** for h in dev.test-domain-12345.com api.test-domain-12345.com; do curl -sI https://$h | head -1; done

Ficha 4

Falta la cabecera X-Frame-Options

10 min · Infraestructura

[Media]

● **Qué riesgo implica:** Sin esta cabecera la web se puede incrustar en un iframe invisible (clickjacking): el usuario pulsa 'Comprar' o 'Aceptar' sin saberlo.

Pasos para resolverlo:
1. Identifica dónde termina el TLS (CDN o servidor propio).
2. Añade la cabecera con el valor SAMEORIGIN.
3. Purga la caché del CDN y comprueba que la respuesta ya la incluye.

Cómo aplicarlo:

```
# Nginx
add_header X-Frame-Options "SAMEORIGIN" always;

# Apache
Header always set X-Frame-Options "SAMEORIGIN"

# Cloudflare (Rules > Transform Rules > Modify Response Header)
Set static  ·  X-Frame-Options: SAMEORIGIN

# IIS (web.config)
<add name="X-Frame-Options" value="SAMEORIGIN" />
```

■ **Verificar:** curl -sI https://test-domain-12345.com | grep -i 'x-frame-options'

Ficha 5

Falta la cabecera X-Content-Type-Options

10 min · Infraestructura

[Media]

● **Qué riesgo implica:** Sin nosniff el navegador puede interpretar un fichero subido como HTML o JavaScript y ejecutarlo (MIME sniffing).

Pasos para resolverlo:
1. Identifica dónde termina el TLS (CDN o servidor propio).
2. Añade la cabecera con el valor nosniff.
3. Purga la caché del CDN y comprueba que la respuesta ya la incluye.

Cómo aplicarlo:

```
# Nginx
add_header X-Content-Type-Options "nosniff" always;

# Apache
Header always set X-Content-Type-Options "nosniff"

# Cloudflare (Rules > Transform Rules > Modify Response Header)
Set static  ·  X-Content-Type-Options: nosniff

# IIS (web.config)
<add name="X-Content-Type-Options" value="nosniff" />
```

■ **Verificar:** curl -sI https://test-domain-12345.com | grep -i 'x-content-type-options'

Ficha 6

robots.txt revela rutas sensibles

20 min · Desarrollo **[Media]**

● **Qué riesgo implica:** robots.txt no protege nada: es una lista pública de lo que NO quieres que se indexe. Poner /admin ahí equivale a publicar la dirección del panel para que la encuentre cualquier escáner.

Pasos para resolverlo:
1. Quita de robots.txt las rutas privadas (/admin, /account, paneles).
2. Protege esas rutas con autenticación real, no con robots.txt.
3. Si el panel debe ser privado, restríngelo por IP o VPN.

Cómo aplicarlo:

```
# robots.txt: solo rutas de indexación, nunca de seguridad
User-agent: *
Disallow: /cart
Disallow: /checkout
# NO pongas aquí /admin ni /account
```

■ **Verificar:** curl -s https://test-domain-12345.com/robots.txt

Ficha 7

Falta la cabecera Referrer-Policy

10 min · Infraestructura **[Baja]**

● **Qué riesgo implica:** Sin política, la URL completa (con tokens o IDs) se filtra en la cabecera Referer a sitios de terceros.

Pasos para resolverlo:
1. Identifica dónde termina el TLS (CDN o servidor propio).
2. Añade la cabecera con el valor strict-origin-when-cross-origin.
3. Purga la caché del CDN y comprueba que la respuesta ya la incluye.

Cómo aplicarlo:

```
# Nginx
add_header Referrer-Policy "strict-origin-when-cross-origin" always;

# Apache
Header always set Referrer-Policy "strict-origin-when-cross-origin"

# Cloudflare (Rules > Transform Rules > Modify Response Header)
Set static  ·  Referrer-Policy: strict-origin-when-cross-origin

# IIS (web.config)
<add name="Referrer-Policy" value="strict-origin-when-cross-origin" />
```

■ **Verificar:** curl -sI https://test-domain-12345.com | grep -i 'referrer-policy'

Ficha 8

Falta la cabecera Permissions-Policy

10 min · Infraestructura **[Baja]**

● **Qué riesgo implica:** Sin esta cabecera, código de terceros embebido puede solicitar cámara, micrófono o ubicación del visitante.

Pasos para resolverlo:
1. Identifica dónde termina el TLS (CDN o servidor propio).
2. Añade la cabecera con el valor geolocation=(), microphone=(), camera=().
3. Purga la caché del CDN y comprueba que la respuesta ya la incluye.

Cómo aplicarlo:

```
# Nginx
add_header Permissions-Policy "geolocation=(), microphone=(), camera=()" al
ways;

# Apache
Header always set Permissions-Policy "geolocation=(), microphone=(), camera
=()"

# Cloudflare (Rules > Transform Rules > Modify Response Header)
Set static  ·  Permissions-Policy: geolocation=(), microphone=(), camera=()

# IIS (web.config)
<add name="Permissions-Policy" value="geolocation=(), microphone=(), camera
=()" />
```

■ **Verificar:** curl -sI https://test-domain-12345.com | grep -i 'permissions-policy'

Ficha 9

Falta la cabecera Cross-Origin-Opener-Policy

10 min · Infraestructura **[Baja]**

● **Qué riesgo implica:** Aísla la ventana de referencias cruzadas (mitigación de Spectre y de ataques de ventana compartida).

Pasos para resolverlo:
1. Identifica dónde termina el TLS (CDN o servidor propio).
2. Añade la cabecera con el valor same-origin.
3. Purga la caché del CDN y comprueba que la respuesta ya la incluye.

Cómo aplicarlo:

```
# Nginx
add_header Cross-Origin-Opener-Policy "same-origin" always;

# Apache
Header always set Cross-Origin-Opener-Policy "same-origin"

# Cloudflare (Rules > Transform Rules > Modify Response Header)
Set static  ·  Cross-Origin-Opener-Policy: same-origin

# IIS (web.config)
<add name="Cross-Origin-Opener-Policy" value="same-origin" />
```

■ **Verificar:** curl -sI https://test-domain-12345.com | grep -i 'cross-origin-opener-policy'

Ficha 10

HSTS no detectado

1 h · Desarrollo / Infraestructura **[Baja]**

● **Qué riesgo implica:** El módulo de ssl analysis lo reporta así: HSTS no detectado

Pasos para resolverlo:
1. Localiza el componente afectado en la configuración actual.
2. Aplica la corrección indicada por el módulo correspondiente.
3. Repite la auditoría y confirma que el hallazgo desaparece.

■ **Verificar:** volver a ejecutar el análisis de test-domain-12345.com

Antes y después de las cabeceras

Lo que devuelve hoy el servidor frente a lo que debe devolver cuando estén aplicadas. Comparación directa para verificar a ojo.

AHORA — lo que devuelve el servidor	DESPUÉS — lo que debe devolver
`Strict-Transport-Security: (ausente)`	`Strict-Transport-Security: max-age=31536000; includeSubDomains`
`Content-Security-Policy: (ausente)`	`Content-Security-Policy: default-src 'self'; object-src 'non…`
`X-Frame-Options: (ausente)`	`X-Frame-Options: SAMEORIGIN`
`X-Content-Type-Options: (ausente)`	`X-Content-Type-Options: nosniff`
`Referrer-Policy: (ausente)`	`Referrer-Policy: strict-origin-when-cross-origin`
`Permissions-Policy: (ausente)`	`Permissions-Policy: geolocation=(), microphone=(), camera=()`
`Cross-Origin-Opener-Policy: (ausente)`	`Cross-Origin-Opener-Policy: same-origin`

● Recon Pipeline

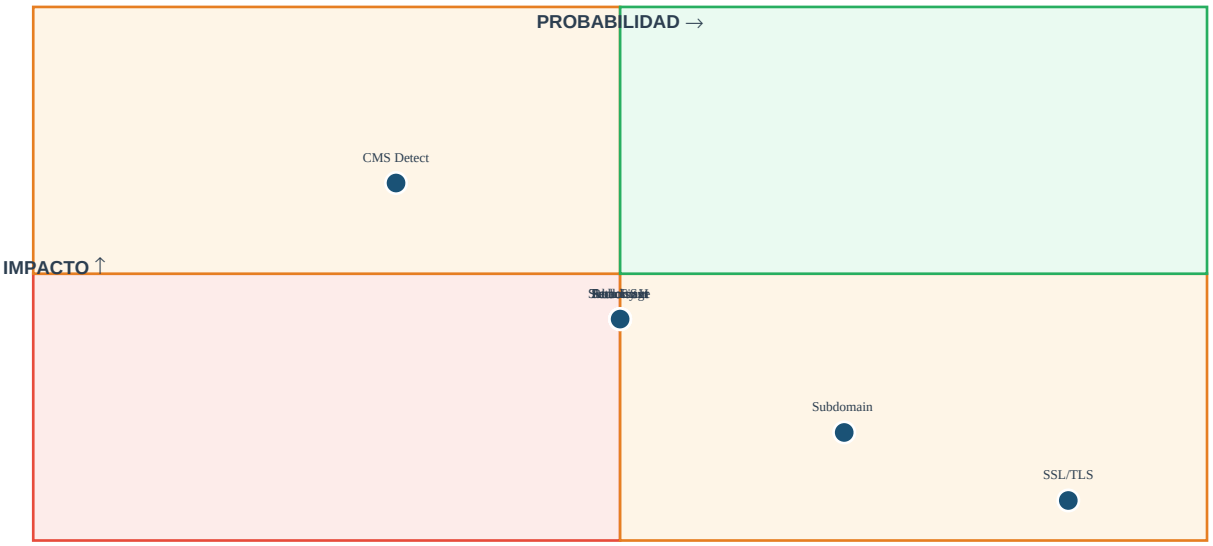
Recon Pipeline [MEDIUM]

● **Qué riesgo implica:** 29 hosts vivos - superficie amplia, priorizar auditoria de los servicios expuestos

Pasos para resolverlo:
1. 29 hosts vivos - superficie amplia, priorizar auditoria de los servicios expuestos

Priorización de Hallazgos

Matriz impacto × probabilidad. Los hallazgos en el cuadrante rojo (alto impacto, alta probabilidad) deben abordarse primero.



Plan de Acción Priorizado

Prioridad	Hallazgo	Severidad	Estado
1	SSL/TLS	CRITICAL	Pendiente
2	Subdomain Takeover	HIGH	Pendiente
3	Threat Intelligence	HIGH	Pendiente
4	Attack Surface	MEDIUM	Pendiente
5	Subdomain Discovery	MEDIUM	Pendiente
6	Tech Fingerprint	MEDIUM	Pendiente
7	Robots.txt Exposure	MEDIUM	Pendiente
8	Security Headers	MEDIUM	Pendiente
9	Shodan InternetDB	MEDIUM	Pendiente
10	Evolución vs anterior	MEDIUM	Pendiente

Checklist de Verificación

Tras aplicar cada corrección, marca la casilla y ejecuta un nuevo análisis para confirmar que el score ha mejorado. La seguridad es un proceso continuo.

■	Conexión SSL/TLS estable y certificado válido

Próximos Pasos

1. **Priorizar**: aborda primero los problemas marcados como Alta prioridad (SPF, DKIM, DMARC).
2. **Ejecutar**: sigue los pasos indicados para cada hallazgo.
3. **Verificar**: tras aplicar los cambios, ejecuta un nuevo análisis con Hermes Security para confirmar que el score ha mejorado.
4. **Repetir**: la seguridad es un proceso continuo. Programa análisis periódicos.

Hermes Security
Contacto: cyberdefense.valencia@proton.me
cybersofia.tech — nuestros servicios y auditorías
Confidencialidad: Esta guía es confidencial y está dirigida únicamente al destinatario.