Correduría Ejemplo

INFORME

Informe de ciberriesgo

Talleres Ejemplo SL

`talleres-ejemplo.example`

Datos del 10 nov 2026, 18:27

E

17 de 100

Riesgo muy alto: hay puertas abiertas a internet que conviene cerrar esta misma semana.

EJEMPLO

Resumen para la dirección

NOTA
E 17 de 100
A: 90-100 · B: 75-89 · C: 60-74 · D: 40-59 · E: menos de 40

HALLAZGOS CRÍTICOS Y ALTOS
4
de 9 hallazgos en total

DÍAS HASTA LA RENOVACIÓN
75
Renueva el 24 ene 2027; contados desde la fecha de los datos

Riesgo muy alto: hay puertas abiertas a internet que conviene cerrar esta misma semana.

De dónde sale la nota

APARTADO	RESTADO
Servicios expuestos a internet	−35 de 35
Correo electrónico	−20 de 25
Programas con fallos conocidos	−10 de 10
Página web y cifrado	−8 de 8
Suplantación del dominio	−6 de 6
Subdominios olvidados	−4 de 4

Evolución de la nota



De 62 (27 oct 2026) a 17 (10 nov 2026), en 3 escaneos.

Lo más importante

GRAVEDAD	QUÉ HEMOS VISTO	PUNTOS QUE RESTA
Crítico	Escritorio remoto o carpetas compartidas visibles desde internet	−20
Crítico	Base de datos o panel de administración expuesto	−15
Alto	El dominio no impide que se envíen correos en su nombre (DMARC)	−12
Alto	La web usa programas con fallos graves conocidos	−10
Medio	No está bien definido quién puede enviar correo del dominio (SPF)	−8

... y 4 más en el plan de acción y en el anexo.

POR DÓNDE EMPEZAR

Cerrar en el cortafuegos los puertos de RDP (3389) y SMB (445, 139) hacia internet. Si hace falta acceso remoto, darlo solo a través de una VPN con doble factor.

Esta nota solo refleja lo que se ve desde internet; el detalle de lo que no cubre está al final.

EJEMPLO

Plan de acción

Qué hacer, por orden. La prioridad sigue la gravedad y los puntos que resta cada problema; el esfuerzo es orientativo.

N.º	QUÉ HACER	QUIÉN	ESFUERZO	PUNTOS QUE SE RECUPERAN
1	● Crítico Cerrar hacia internet los puertos de escritorio remoto y carpetas compartidas; el acceso remoto, solo por VPN con doble factor.	Informático	Horas	+20
2	● Crítico Dejar la base de datos y los paneles de administración accesibles solo desde la red interna o por VPN.	Informático	Horas	+15
3	● Alto Publicar un registro DMARC con política de cuarentena o rechazo.	Informático	Horas	+12
4	● Alto Actualizar el gestor de contenidos de la web y sus complementos a versiones con soporte.	Proveedor web	Días	+10
5	● Medio Corregir el registro SPF para que solo envíen correo los servidores autorizados.	Informático	Horas	+8
6	● Medio Avisar al equipo y a los clientes de los dominios parecidos y valorar reclamarlos o denunciarlos.	Dirección	Días	+6
7	● Medio Renovar o corregir el certificado de la web y forzar siempre la conexión cifrada.	Proveedor web	Horas	+5
8	● Bajo Dar de baja los subdominios que ya no se usan y los servicios que apuntan a ellos.	Informático	Horas	+4
9	● Bajo Añadir las cabeceras de seguridad que faltan en la configuración de la web.	Proveedor web	Horas	+3

Cada cifra es lo que subiría la nota si se resolviera solo ese problema; al tener cada apartado un tope, no siempre coincide con lo que resta ni se pueden sumar sin más.

C 74 Si se resuelven los problemas críticos y altos, la nota pasaría de 17 a 74 sobre 100 y la letra sería C.

EJEMPLO

Anexo técnico para el responsable de informática

Crítico — Escritorio remoto o carpetas compartidas visibles desde internet

`exposure.remote_access` −20 puntos

QUÉ ES

Cualquiera en internet puede llegar a la puerta de entrada de los ordenadores o de las carpetas compartidas de la empresa.

POR QUÉ IMPORTA

Es la vía de entrada más habitual de los ataques con secuestro de datos (ransomware): los delincuentes prueban contraseñas hasta entrar y cifran todo.

QUÉ HEMOS VISTO EXACTAMENTE

- Puerto 3389 (RDP) abierto en `198.51.100.23`, visto por última vez el 5 nov 2026; localizado a través del subdominio `remoto.talleres-ejemplo.example`.

CÓMO SE ARREGLA

Cerrar en el cortafuegos los puertos de RDP (3389) y SMB (445, 139) hacia internet. Si hace falta acceso remoto, darlo solo a través de una VPN con doble factor.

Crítico — Base de datos o panel de administración expuesto

`exposure.database_admin` −15 puntos

QUÉ ES

Una base de datos o un panel para administrar sistemas está accesible desde internet.

POR QUÉ IMPORTA

Ahí están los datos de clientes y el control de los sistemas. Si alguien entra, puede copiar o borrar la información y la empresa tendría que notificarlo.

QUÉ HEMOS VISTO EXACTAMENTE

- MySQL accesible en `198.51.100.23`, puerto 3306, visto por última vez el 6 nov 2026; localizado a través del dominio.

CÓMO SE ARREGLA

Dejar la base de datos y los paneles (phpMyAdmin, Adminer, pgAdmin, administración del router o del cortafuegos) accesibles solo desde la red interna o por VPN. Revisar que tengan contraseña robusta y doble factor.

Alto — El dominio no impide que se envíen correos en su nombre (DMARC)

`email.dmarc` −12 puntos

QUÉ ES

Cualquiera puede enviar correos que parecen venir de la empresa, y los servidores de correo de los destinatarios no tienen instrucciones para rechazarlos.

POR QUÉ IMPORTA

Es la base de los fraudes de facturas falsas y de cambio de cuenta bancaria: clientes y proveedores reciben un correo que parece legítimo.

QUÉ HEMOS VISTO EXACTAMENTE

- El dominio no publica ningún registro DMARC.

CÓMO SE ARREGLA

Publicar un registro DMARC en _dmarc.<dominio> con política quarantine o reject (no basta con `p=none`). Empezar por `p=none` con informes (rua) solo durante unas semanas para revisar quién envía, y después endurecer.

Alto — La web usa programas con fallos graves conocidos

`software.vulnerable` −10 puntos

QUÉ ES

El gestor de contenidos de la web, o alguna de sus piezas, muestra una versión exacta para la que hay publicados fallos de seguridad graves.

POR QUÉ IMPORTA

Los fallos públicos se explotan de forma automática. Una web comprometida puede robar datos de formularios, mostrar contenido fraudulento o infectar a quien la visita.

QUÉ HEMOS VISTO EXACTAMENTE

- drupal versión `9.3.0`, con estos avisos de seguridad graves: `CVE-2022-25277`.

CÓMO SE ARREGLA

Actualizar el CMS, sus plugins y librerías a versiones con soporte. Activar las actualizaciones automáticas de seguridad y retirar lo que no se use.

EJEMPLO

Medio — No está bien definido quién puede enviar correo del dominio (SPF)

`email.spf` −8 puntos

QUÉ ES

Falta, o está mal configurada, la lista de servidores autorizados a enviar correo en nombre de la empresa.

POR QUÉ IMPORTA

Sin esa lista es más fácil suplantar a la empresa, y sus correos legítimos acaban con más frecuencia en la carpeta de correo no deseado.

QUÉ HEMOS VISTO EXACTAMENTE

- El dominio no publica ningún registro SPF.

CÓMO SE ARREGLA

Publicar un único registro TXT SPF que incluya solo a los proveedores que envían correo y termine en -all o ~all, sin superar las 10 consultas DNS.

Medio — Hay dominios recientes casi iguales al de la empresa con correo o web en marcha

`lookalike.active` −6 puntos

QUÉ ES

En los últimos doce meses alguien ha registrado dominios que se confunden a simple vista con el de la empresa y los tiene preparados para enviar correo o mostrar una web.

POR QUÉ IMPORTA

Se usan para engañar a clientes, proveedores y empleados con correos o páginas que parecen de la empresa.

QUÉ HEMOS VISTO EXACTAMENTE

- `talleres-ejemp1o.example`, registrado el 14 ago 2026.

CÓMO SE ARREGLA

Revisar la lista de dominios. Si no son de la empresa, avisar a empleados y clientes, bloquearlos en el filtro de correo y valorar pedir su retirada al registrador.

Medio — La web no protege bien la conexión (HTTPS)

`web.tls` −5 puntos

QUÉ ES

La web no tiene conexión segura, no obliga a usarla, tiene el certificado caducado o acepta un cifrado antiguo.

POR QUÉ IMPORTA

Lo que escriben los visitantes (formularios, contraseñas) puede leerse o modificarse por el camino, y los navegadores muestran la web como «no segura».

QUÉ HEMOS VISTO EXACTAMENTE

- El certificado de la web está caducado (venció el 1 oct 2026).

CÓMO SE ARREGLA

Instalar un certificado válido con renovación automática, redirigir todo el tráfico de HTTP a HTTPS y desactivar TLS 1.0 y 1.1 (dejar TLS 1.2 y 1.3).

Bajo — Hay subdominios con servicios que parecen olvidados

`subdomains.forgotten` −4 puntos

QUÉ ES

Existen direcciones antiguas de la empresa (pruebas, versiones viejas de la web) que siguen publicadas.

POR QUÉ IMPORTA

Lo que nadie mantiene no se actualiza, y suele ser el punto más débil.

QUÉ HEMOS VISTO EXACTAMENTE

- `antiguo.talleres-ejemplo.example` sigue publicado y responde.

CÓMO SE ARREGLA

Revisar la lista de subdominios, apagar los que no se usen y borrar sus registros DNS. Mantener un inventario de lo que está publicado.

Bajo — A la web le faltan protecciones básicas del navegador

`web.security_headers` −3 puntos

QUÉ ES

La web no envía las instrucciones de seguridad que los navegadores usan para proteger a quien la visita.

POR QUÉ IMPORTA

Sin ellas son más fáciles algunos engaños, como incrustar la web dentro de otra página o inyectar contenido ajeno.

QUÉ HEMOS VISTO EXACTAMENTE

- Faltan estas cabeceras de seguridad: content-security-policy.

CÓMO SE ARREGLA

Añadir las cabeceras Strict-Transport-Security, Content-Security-Policy, X-Content-Type-Options y X-Frame-Options (o frame-ancestors) en el servidor web.

EJEMPLO

Alcance, fuentes y método

No se pudo comprobar

Esto no resta puntos, pero tampoco está comprobado que esté bien.

- **Firma de los correos (DKIM).** No hemos encontrado la firma DKIM en los selectores habituales; pídele el selector a tu informático.

Lo que esta nota no ve

- Cómo se trabaja por dentro: contraseñas, permisos y quién tiene acceso a qué.
- La formación de los empleados frente a correos y llamadas fraudulentas.
- Si existen copias de seguridad y si se ha probado a recuperarlas.
- Los ordenadores, móviles y redes internas, que no son visibles desde internet.
- Solo vemos los servicios que cuelgan del dominio de la empresa o de las direcciones que nos indiques; una oficina sin nombre asociado no aparece.
- Los servicios en la nube que no cuelgan del dominio de la empresa.

Fuentes de datos

Consultas DNS y una visita normal a la web de la empresa. No se usaron datos de terceros.

Metodología

1. Observación externa y pasiva: consultas DNS, registros públicos de certificados, datos ya recogidos por terceros y una visita normal a la web.
2. No se ha realizado ninguna prueba intrusiva ni se ha accedido a ningún sistema de la empresa.
3. La nota parte de 100 y resta puntos según reglas públicas; cada punto restado corresponde a una regla y a lo que se observó.
4. Versión de las reglas: v0.6.
5. Fecha de los datos: 10 nov 2026, 18:27.

Escaneo terminado el 10 nov 2026, 18:27 · Informe generado el 11 nov 2026, 12:15

EJEMPLO