

ARGUS NODO

Postura de seguridad medida y firmada

Informe de Postura de Seguridad

Activo	metrocoord.duckdns.org
URL	https://metrocoord.duckdns.org
Fecha	2026-10-27 03:26 UTC
Analista	Analista de seguridad
Alcance	Solo lectura, externo. Nuclei (plantillas firmadas) + cabeceras HTTP + TLS + DNS + puertos.
Firma	SHA-256 del PDF + timestamp (integridad, no PKI)

81

PUNTUACION DE POSTURA

ACCEPTABLE

10 hallazgos en total. 1 por encima de Priority 50 (accion en el trimestre).

Resumen por severidad

Severidad	Hallazgos	Notas
MEDIUM	1	Arreglar este trimestre
LOW	3	Planificar
INFO	6	Monitorizar / aceptar
Total	10	

Los tres mas urgentes

#	Hallazgo	Severidad	Priority	Plazo
F-001	Sin SPF ni DMARC en un dominio con MX activos	MEDIUM	59	Arreglar este trimestre
F-002	Falta /.well-known/security.txt (RFC 9116)	LOW	36	Planificar
F-007	Version de OpenSSH expuesta en el banner de SSH	LOW	36	Planificar

Quick Wins

#	Hallazgo	Esfuerzo	Priority
F-001	Sin SPF ni DMARC en un dominio con MX activos	15 min	59
F-002	Falta /.well-known/security.txt (RFC 9116)	15 min	36
F-007	Version de OpenSSH expuesta en el banner de SSH	15 min	36
F-003	robots.txt y sitemap.xml devuelven el HTML de la SPA en vez de su contenido	15 min	35

Superficie de ataque

```
graph TD
    User((Usuario)) -->|HTTPS 443| N["nginx catch-all  
ssl_reject_handshake + 444"]
    Attacker((Atacante)) -.->|escaneo| N
    N -->|Host permitido| FE["frontend SPA"]
    N -->|/api/| BE["backend FastAPI :8000"]
    BE --> DB[(PostgreSQL 16)]
    BE --> RD[(Redis 7)]
    Wild((*.metrocoord.duckdns.org DNS wildcard)) -.-> N
```

Puertos expuestos a Internet: 22/tcp, 80/tcp, 443/tcp | **Filtrados:** 20 de los puertos habituales.

F-001 | Sin SPF ni DMARC en un dominio con MX activos

MEDIUM **Priority 59/100** Arreglar este trimestre

OWASP 2025	A05:2025 - Security Misconfiguration
CWE	CWE-284
CVSS	5.3
EPSS	n/a (sin CVE)
CISA KEV	no
Exposicion	6/10
Confianza	95%
Puntuacion	base por severidad (sin CVE)
Fuente	Analisis manual sobre evidencia

Evidencia

Confirmado de forma independiente por el motor: la plantilla txt-fingerprint tambien devuelve un registro TXT vacio.

```
dig +short metrocoord.duckdns.org TXT      -> (vacio)
dig +short _dmarc.metrocoord.duckdns.org TXT -> (vacio)
dig +short metrocoord.duckdns.org MX       -> 9 registros MX activos
```

El dominio tiene 9 registros MX (DuckDNS) que enrutan correo entrante, pero no declara que emisores son legitimos (SPF) ni que hacer con los que no lo son (DMARC).
Un atacante puede enviar correo con From: <cualquiera@metrocoord.duckdns.org> y el mensaje llegara a los buzones que no apliquen DMARC.

Riesgo. Suplantacion de identidad del dominio (phishing y fraude con remitente creible) y amplificacion de spam. Impacto sobre la reputacion de la marca y sobre los clientes que confien en el dominio.

Remediacion. Anadir un registro TXT con SPF delphi del proveedor real, y publicar _dmarc.metrocoord.duckdns.org TXT "v=DMARC1; p=none; rua=mailto:postmaster@..." empezando por p=none (modo monitor) y subir a p=quarantine tras 2 semanas.

F-002 | Falta /.well-known/security.txt (RFC 9116)

LOW

Priority 36/100

Planificar

OWASP 2025	A09:2025 - Security Logging and Alerting Failures
CWE	CWE-16
CVSS	2.1
EPSS	n/a (sin CVE)
CISA KEV	no
Exposicion	5/10
Confianza	100%
Puntuacion	base por severidad (sin CVE)
Fuente	Analisis manual sobre evidencia

Evidencia

```
GET /.well-known/security.txt -> HTTP 404 (146 bytes)
```

Un tercero que detecte una vulnerabilidad en el activo no tiene un canal oficial para reportarla, y acabaria publicandola sin aviso.

Riesgo. El canal de reporte se pierde: incrementan los hallazgos publicados sin control y se pierde trazabilidad.

Remediacion. Publicar /.well-known/security.txt con Contact:, Expires:, Preferred-Languages: y Encryption:. Servirlo desde el nginx con un location propio (no desde la SPA).

F-007 | Version de OpenSSH expuesta en el banner de SSH

LOW **Priority 36/100** Planificar

OWASP 2025	A05:2025 - Security Misconfiguration
CWE	CWE-200
CVSS	3.1
EPSS	n/a (sin CVE)
CISA KEV	no
Exposicion	5/10
Confianza	100%
Puntuacion	base por severidad (sin CVE)
Fuente	Nuclei 3.11.1 (motor del VPS)

Evidencia

Plantilla nuclei: ssh-server-enumeration
Banner observado: metrocoord.duckdns.org:22

El servidor anuncia su version exacta y el parche de Ubuntu. Eso permite a quien ataca elegir exploits publicos para esa version exacta sin enumerar nada.

Riesgo. Facilita el acoplamiento de exploits publicos al servidor (reduccion del trabajo de reconocimiento).

Remediacion. Ajustar /etc/ssh/sshd_config: De banner /etc/ssh/sshd_config.d/ y dejar solo #VersionAddendum (sin texto de version). Revisar que fail2ban siga leyendo los logs.

F-003 | robots.txt y sitemap.xml devuelven el HTML de la SPA en vez de su contenido

LOW

Priority 35/100 Planificar

OWASP 2025	A02:2025 - Security Misconfiguration
CWE	CWE-441
CVSS	2.0
EPSS	n/a (sin CVE)
CISA KEV	no
Exposicion	4/10
Confianza	95%
Puntuacion	base por severidad (sin CVE)
Fuente	Analisis manual sobre evidencia

Evidencia

```
GET /robots.txt      -> HTTP 200, 681 bytes
GET /sitemap.xml    -> HTTP 200, 681 bytes
GET /               -> HTTP 200, 681 bytes
```

Los tres devuelven exactamente el mismo cuerpo (index.html de la SPA).
El catch-all de nginx sirve el frontend para cualquier ruta.

Riesgo. Los crawlers interpretan HTML como robots.txt: indexacion de rutas que no existen, ruido en los buscadores y perdida de las directivas reales de rastreo.

Remediacion. Anadir en el vhost locations especificos que devuelvan 404 (o el fichero real) para /robots.txt y /sitemap.xml, en lugar de caer en el fallback de la SPA.

F-008 | El banner SSH ofrece el algoritmo de firma SHA1

INFO **Priority 14/100** Monitorizar / aceptar

OWASP 2025	A02:2025 - Security Misconfiguration
CWE	CWE-327
CVSS	2.0
EPSS	n/a (sin CVE)
CISA KEV	no
Exposicion	5/10
Confianza	95%
Puntuacion	base por severidad (sin CVE)
Fuente	Nuclei 3.11.1 (motor del VPS)

Evidencia

```
Plantilla nuclei: ssh-sha1-hmac-algo
Host: metrocoord.duckdns.org:22
```

OpenSSH anuncia tambien un algoritmo de firma basado en SHA-1, considerado obsoleto para firmas.

Riesgo. Un atacante que controle la negociacion podria forzar un algoritmo mas debil. Impacto practico bajo en OpenSSH moderno.

Remediacion. Configurar HostKeyAlgorithms en sshd_config dejando solo algoritmos con SHA-2 o superiores, y verificar la compatibilidad con los clientes.

F-010 | Tecnología del servidor web revelada

INFO **Priority 14/100** Monitorizar / aceptar

OWASP 2025	A05:2025 - Security Misconfiguration
CWE	CWE-200
CVSS	1.5
EPSS	n/a (sin CVE)
CISA KEV	no
Exposicion	5/10
Confianza	100%
Puntuacion	base por severidad (sin CVE)
Fuente	Nuclei 3.11.1 (motor del VPS)

Evidencia

```
Plantilla nuclei: tech-detect:nginx
Cabecera Server: nginx
```

Tambien se expone la version exacta de OpenSSH en el banner de SSH (F-007).

Riesgo. Reduce el esfuerzo de reconocimiento del atacante. Bajo impacto por si solo.

Remediacion. Usar server_tokens off; en nginx y ocultar el banner de SSH (De banner /etc/ssh/sshd_config.d/).

F-004 | Sin registro CAA (ninguna CA esta autorizada a emitir)

INFO **Priority 13/100** Monitorizar / aceptar

OWASP 2025	A02:2025 - Security Misconfiguration
CWE	CWE-284
CVSS	1.0
EPSS	n/a (sin CVE)
CISA KEV	no
Exposicion	4/10
Confianza	100%
Puntuacion	base por severidad (sin CVE)
Fuente	Analisis manual sobre evidencia

Evidencia

```
dig +short metrocoord.duckdns.org CAA -> (sin registro)
```

Sin CAA, cualquier CA del ecosistema puede emitir un certificado para el dominio.

Riesgo. Un CCA comprometido o malicioso puede emitir certificados validos para el dominio (phishing con HTTPS creible).

Remediacion. Publicar CAA con las CA realmente usadas (p. ej. "letsencrypt.org") y marcar issuewild como no.

F-005 | DNS wildcard activo: cualquier subdominio resuelve a este servidor

INFO **Priority 13/100** Monitorizar / aceptar

OWASP 2025	A05:2025 - Security Misconfiguration
CWE	CWE-441
CVSS	2.0
EPSS	n/a (sin CVE)
CISA KEV	no
Exposicion	4/10
Confianza	90%
Puntuacion	base por severidad (sin CVE)
Fuente	Análisis manual sobre evidencia

Evidencia

```
nuclei -t dns -> [wildcard-dns-detect] *.metrocoord.duckdns.org -> 2.24.73.87
```

Comprobado: un subdominio aleatorio resuelve a la IP del servidor.
crt.sh no registra subdominios para el dominio (historial de CT vacío).

Riesgo. Superficie de ataque ampliada sin control: infinitos hostnames apuntan al servidor. Facilita phishing con subdominio creíble y ensucia los logs de CT y los certificados.

Remediación. Si el wildcard no es necesario, desactivarlo en el panel de DuckDNS. Si se mantiene, servir un catch-all estricto (lo que ya hace nginx: 444 y ssl_reject_handshake) y vigilar los nuevos nombres en crt.sh cada mes.

F-009 | Cabecera X-XSS-Protection obsoleta presente

INFO **Priority 13/100** Monitorizar / aceptar

OWASP 2025	A02:2025 - Security Misconfiguration
CWE	CWE-16
CVSS	1.0
EPSS	n/a (sin CVE)
CISA KEV	no
Exposicion	4/10
Confianza	100%
Puntuacion	base por severidad (sin CVE)
Fuente	Nuclei 3.11.1 (motor del VPS)

Evidencia

Plantilla nuclei: xss-deprecated-header
Valor observado: <https://metrocoord.duckdns.org>

El filtro XSS de los navegadores antiguos fue retirado del estandar y su implementacion en algunos navegadores introducía sus propios problemas.

Riesgo. Ruido de cabeceras, sin impacto real en los navegadores actuales. En algunos navegadores antiguos el filtro pouvait introducir vulnerabilidades.

Remediacion. Eliminar la cabecera X-XSS-Protection. La proteccion real la aporta la CSP, que ya esta presente.

F-006 | Cabeceras de aislamiento de origen ausentes (4)

INFO

Priority 13/100

Monitorizar / aceptar

OWASP 2025	A05:2025 - Security Misconfiguration
CWE	CWE-693
CVSS	1.5
EPSS	n/a (sin CVE)
CISA KEV	no
Exposicion	4/10
Confianza	100%
Puntuacion	base por severidad (sin CVE)
Fuente	Nuclei 3.11.1 (motor del VPS)

Evidencia

Detectado por el motor (plantilla http-missing-security-headers):

- X-Permitted-Cross-Domain-Policies
- Cross-Origin-Embedder-Policy (COEP)
- Cross-Origin-Opener-Policy (COOP)
- Cross-Origin-Resource-Policy (CORP)

Las cabeceras de cross-origin aislan el documento de otros orígenes. COOP y CORP ya son parte de la práctica estándar; COEP solo aplica a documentos que usan SharedArrayBuffer (aislamiento fuerte).

Riesgo. Ausencia de una capa de aislamiento entre orígenes: menos defence-in-depth frente a XS-Leak y ataques de cross-origin.

Remediación. Anadir en el vhost de nginx: add_header Cross-Origin-Opener-Policy "same-origin" always; add_header Cross-Origin-Resource-Policy "same-origin" always; add_header X-Permitted-Cross-Domain-Policies "none" always; (COEP solo si la aplicación lo necesita)

Lo que ya está bien

Control	Estado	Por que importa
Puertos expuestos	Solo 3 puertos publicos (22/tcp, 80/tcp, 443/tcp). 20 puertos habituales filtrados.	Superficie minima. No hay RDP, VNC, SQL, Redis ni paneles de administracion accesibles desde internet.
TLS	TLS 1.3 con cifrado AEAD (AES-256/SHA-384), sin suites CBC. Certificado Let's Encrypt valido, 65 dias restantes.	Cifrado moderno y renovacion automatizada. Solo las suites AEAD evitan los ataques de padding oracle.
Cabeceras de seguridad	Presentes CSP, HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy y Permissions-Policy.	El CSP es restrictivo (default-src 'self') y el HSTS con

		includeSubDomains.
Huella tecnica	Sin cabecera X-Powered-By: no se revela la tecnologia del backend.	Reduce la informacion que el atacante obtiene antes de atacar.
Filtrado de Host	El catch-all cierra los hosts desconocidos con 444 y rechaza el handshake TLS con ssl_reject_handshake.	Impide el escaneo por IP desnuda y el ataque de inyeccion de Host (CWE-113).
Superficie de certificados	crt.sh no registra subdominios para el dominio.	No hay historial de nombres de confianza que exponer.
WAF Detection	Se detecta una capa de proxy o WAF delante de la aplicacion: el trafico no llega directo al backend, sino a un filtrado que responde con 444 y rechaza el handshake TLS en hosts desconocidos.	Detectado de forma independiente por el motor de escaneo.
SSH Auth Methods - Detection	SSH con autenticacion solo por clave publica: el servidor anuncia unicamente el metodo publickey. La autenticacion por password esta deshabilitada en el servidor (PasswordAuthentication no).	Detectado de forma independiente por el motor de escaneo.
ACME DNS Challenge - Detect	El proceso de emision de certificados esta automatizado: el reto ACME se resuelve sin intervencion manual.	Detectado de forma independiente por el motor de escaneo.

Diff de auditoria

Primer informe de la serie. No existe todavia un informe previo con el que comparar.

A partir del siguiente ciclo, este informe incluira la comparativa: arreglados, hallazgos nuevos, todavia presentes y puntuacion de progreso.

Apendice - Metodologia y limitaciones

```
nuclei 3.11.1 -u https://metrocoord.duckdns.org -t /root/nuclei-templates
               -severity critical,high,medium,low,info
               -exclude-tags dos,intrusive,fuzzing,fuzz,headless,code,file,oast,bruteforce,workflow
               -rate-limit 15 -c 2 -timeout 10 -retries 1 -duc -dut -irr
curl          -sIkL (cabeceras/TLS), -s (descubrimiento)
SslStream    certificado, protocolo, cipher
dig          A AAAA MX NS TXT CAA CNAME
TCP connect  22 puertos habituales
crt.sh       historico de Transparency
```

Garantias: solo lectura; ninguna peticion de escritura; plantillas firmadas unicamente; ritmo limitado a 15 req/s y concurrencia 2.

Limitaciones: sin ZAP passive (demonio Docker local no operativo en el momento); sin pruebas de credenciales por defecto ni de la logica de autenticacion; sin analisis de codigo fuente (el alcance es el activo desplegado); un unico

punto de vista y un unico momento temporal.