

rescue-devsecops · pipeline #1842

```
$ git push origin feature/login
```

```
▶ devsecops-scan    ✓ gitleaks      0 secretos
                   ✓ sbom          CycloneDX 1.6
                   ✓ ai-sast       2 hallazgos · medio
▶ security/gate     ✓ aprobado
▶ build-image       ✓ trivy        sin críticos
▶ gitops-sync       ✓ k8s/produccion
▶ evidencia         ✓ firmada Ed25519
```

FICHA TÉCNICA RESCUE DEVSECOPS

Del commit al clúster, con evidencia ISO 27001.



T.I. RESCUE
SEGURIDAD INFORMÁTICA

ISO 9001

Seguridad informática premium, respaldada por el reconocimiento internacional ISO 9001.



SC-CER900888

ISO 27001

Defendiendo tus datos con rigor internacional: certificación ISO/IEC 27001.



SI-CER900889

ISO 20000-1

Excelencia en gestión de servicios de TI, fundamentada en estándares mundiales de calidad.



TI-CER988544

ISO 22301

Continuidad del negocio sin interrupciones, conforme a estándares internacionales.



CO-CNCER988779

CUATRO CERTIFICACIONES ISO DEFINEN NUESTRA SUPERIORIDAD

Nuestro compromiso con la ciberseguridad trasciende la simple retórica. Es tangible y está validado por cuatro prestigiosas certificaciones **ISO 9001, 27001, 20000-1 y 22301**. No son solo siglas: son el testimonio de nuestra dedicación a ofrecer servicios de primera clase y representan nuestra promesa de calidad, seguridad, **eficiencia y resiliencia**. Al elegirnos no solo escoges un proveedor de ciberseguridad, sino un aliado certificado que entiende y cumple los más altos estándares internacionales.

COMPROMISO INTEGRAL: MÁS ALLÁ DE LA SEGURIDAD BÁSICA

Con nuestras certificaciones garantizamos **calidad, seguridad de la información, excelencia en TI y continuidad del negocio**. Representan nuestro compromiso, profesionalismo e integridad. Elegirnos es optar por una ciberseguridad de élite y con respaldo.



SC-CER900888

SI-CER900889

TI-CER988544

CO-CNCER988779

SOMOS UN ALIADO ESTRATÉGICO

Para la seguridad informática e
infraestructura tecnológica de las
empresas.

EMPRESA FUNDADA EN 2015 CON BASE EN COLOMBIA

Con operación en **todo el mundo**

MISIÓN

Nos especializamos en el soporte y la seguridad informática con los más altos estándares internacionales, incluidas las normas **ISO 9001, 27001, 22301 y 20000-1**. Nuestra misión es garantizar la continuidad operativa de empresas de todos los tamaños con soluciones tecnológicas eficientes y seguras, y servicios personalizados que se ajustan a las necesidades de cada cliente, **evitando interrupciones y promoviendo su éxito.**

VISIÓN

Ser líderes globales en administración y seguridad informática, con soluciones personalizadas y eficientes que garanticen la continuidad operativa. Estamos comprometidos con **la innovación y el cumplimiento de los estándares de calidad y seguridad más rigurosos**, para ser siempre la primera opción de nuestros clientes.

Contáctanos
info@tirescue.com.co
www.tirescue.com

TU SEGURIDAD, NUESTRA PRIORIDAD

Soluciones adaptadas

A la medida de cada cliente, sin importar si la empresa es pequeña o grande.

Actualización constante

Soluciones inmediatas para prevenir pérdidas de información e ir siempre un paso adelante.

Comunicación directa

Sin filas ni turnos.

Ahorro en hardware

Lo que se implementa en software.

Soporte 24/7

Acompañamiento permanente cuando lo necesitas.

Personal atento

Un equipo certificado que conoce tu operación.

NUESTROS VALIOSOS CLIENTES

Asociaciones basadas en la confianza y la excelencia



SILK DUBAI



Grupo OET

Alevilla



ipanū

Oral-Plus
SALUD Y BELLEZA EN TU SONRISA



anquímico

Ame

juju
Soluciones amigables

Clínica mery álvarez
-Desde 1999-



PKF Integral

LLERAS PARK
HOTEL

AUDITORÍAS
E INFORMES

Ame

Empresatur
Más que Transporte

hra

Grupo Agrosiete
S.A.S.

COOPEVIAN
SEGURIDAD PRIVADA

HA
Bicicletas



SP
Soluciones & Partes
S.A.S.

TELSAT

Sary

PLATAFORMA DEVSECOPS

TODO EN UNO · MULTI-CLIENTE



CONCEPTO FUNDAMENTAL DESARROLLO SEGURO DE PUNTA A PUNTA

Rescue DevSecOps reúne en una sola plataforma todo el ciclo de vida del software. Allí se aloja el código, se ejecutan los pipelines, se detectan y gestionan las vulnerabilidades, se publican las imágenes y se despliega en Docker o Kubernetes.

Cada paso deja **evidencia verificable** para los controles de desarrollo seguro de **ISO/IEC 27001:2022**. Seguridad y cumplimiento dejan de ser una tarea aparte: ocurren solos mientras el equipo trabaja.

Está diseñada para operar varios clientes desde una sola instalación, con aislamiento entre ellos y la interfaz en español.

Hosting **Git**

Repositorios, pull requests e issues con ramas protegidas.

Pipelines **CI**

Runner Docker endurecido y logs en vivo.

Seguridad con **IA**

AI-SAST, secretos, SBOM y gate de seguridad en cada PR.

Registro de **imágenes**

Escaneo Trivy automático al publicar.

Despliegue y **GitOps**

Docker y Kubernetes, incluso detrás de NAT.

Evidencia **ISO** **27001**

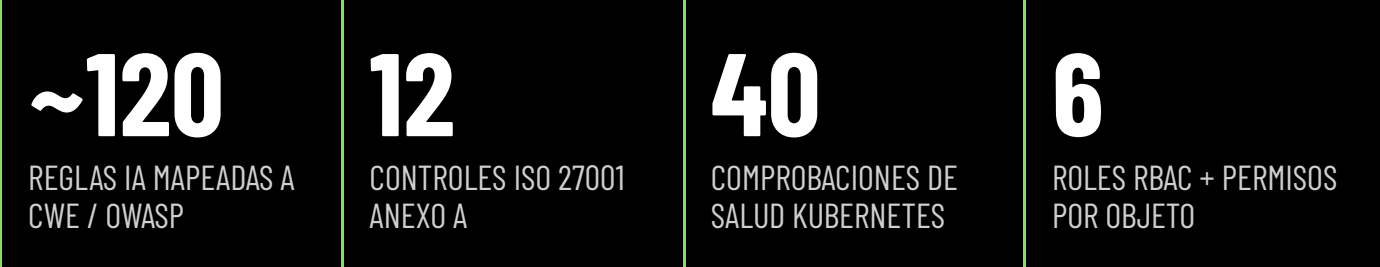
Registro inmutable y firmado, listo para auditoría.

UNA PLATAFORMA, SEIS HERRAMIENTAS MENOS

Cada herramienta extra suma un login, un servidor que mantener y una integración que se rompe. Rescue DevSecOps reúne esas capacidades en un solo producto, con un único modelo de usuarios, permisos y evidencia.



Herramientas cuyas funciones cubre la plataforma. Las marcas pertenecen a sus respectivos titulares.



ASÍ FLUYE UN CAMBIO



HOSTING GIT PARA EQUIPOS QUE ENTREGAN SEGURO

Repositorios Git

Hosting sobre HTTP inteligente, con todo lo que el equipo usa a diario:

- Ramas protegidas y hooks
- Forks y Git LFS
- Releases
- Navegador de código con *blame* y *diff*

Pull requests e issues

Revisiones y checks de estado obligatorios antes de fusionar. Cinco estrategias de merge:

- Merge y squash
- Rebase y rebase-merge
- Fast-forward only

Aprovisionamiento en un formulario

Un repositorio nuevo nace listo con el perfil **devsecops-standard**:

- Ramas **main**, **QA** y **develop** protegidas
- 8 etiquetas y los pipelines de seguridad
- Renovate activo

API compatible con Gitea

Expone **/api/v1** compatible con Gitea, así que Renovate y los scripts existentes funcionan sin cambios. La API nativa REST está documentada con OpenAPI.

Migración desde Gitea

Importa en un solo paso usuarios, contraseñas, 2FA, repositorios, issues, PR, secretos e imágenes. El equipo sigue trabajando sin reconfigurar nada.

Webhooks firmados

Integraciones salientes con firma **HMAC-SHA256** (X-Hub-Signature-256), para que el receptor verifique que el evento es auténtico.

Flujo de trabajo seguro por defecto

Los desarrolladores trabajan con **fork + pull request hacia QA**. Nadie hace *push* directo a **main**, y cada cambio a producción pasa por revisión, pipeline y gate de seguridad.

MOTOR CI PROPIO PIPELINES DEVSECOPS

Cada push dispara el pipeline **devsecops-scan**. Busca secretos con Gitleaks, genera el SBOM, ejecuta el análisis estático con IA y publica el resultado como check del pull request. Hay plantillas listas para construir imágenes (**build-image**) y para proponer correcciones automáticas (**ai-security-fix**).

BOTS DE SEGURIDAD AI-SAST CON CRITERIO DE AUDITOR

- ~18 prompts y ~120 reglas mapeadas a CWE, OWASP e ISO 27001.
- Verificación de falsos positivos antes de reportar.
- Calibración CVSS 3.1 de cada hallazgo.
- Auto-fix por pull request: la corrección también pasa por el gate.
- Chat de triage para discutir un hallazgo con la IA.
- Los secretos se **enmascaran** antes de enviar código al modelo.
- Funciona con el servicio LLM de T.I. RESCUE.

Panel «Calidad IA»

Mide la precisión de los bots y muestra la evolución de los hallazgos por repositorio.

RUNNER ENDURECIDO

Sin privilegios

Capacidades eliminadas (cap_drop ALL) y no-new-privileges.

Límites de recursos

CPU, memoria y PIDs acotados por cada job.

Red aislada

Aislamiento de red y lista de registries permitidos.

Tokens efímeros

Un RunToken por ejecución y secretos enmascarados en los logs.

Pipelines como datos

Plantillas reutilizables, compatibles con *act* y con logs en vivo.

Hallazgos y gates

Todos los escáneres alimentan un único inventario de hallazgos: se deduplican, se priorizan y se les da seguimiento hasta el cierre. El check **security/gate** bloquea el merge cuando hay riesgos fuera de política.

- Aceptación de riesgo formal y trazable
- Exportación **SARIF 2.1.0**
- Importa resultados de SARIF, Semgrep, Bandit, Gitleaks y Trivy

SLA DE REMEDIACIÓN POR SEVERIDAD



SCA y SBOM

Inventario de dependencias en **CycloneDX 1.6** y vulnerabilidades consultadas en **OSV**. Las políticas se apoyan en datos de explotación real para priorizar lo que importa.

- Catálogo **CISA KEV** (vulnerabilidades explotadas)
- Probabilidad de explotación **EPSS**
- Detección de licencias copyleft
- Declaraciones **VEX** y métricas de riesgo por proyecto

Dependencias al día

Renovate integrado abre pull requests de actualización hacia la rama **QA**, que pasan por el mismo pipeline y gate que cualquier otro cambio.

Formatos y fuentes que entiende



DEL REGISTRO AL CLÚSTER

Registro de contenedores

Registro compatible con CNCF Distribution sobre almacenamiento S3. Los tokens **JWT RS256** los emite la plataforma, cada imagen se escanea con **Trivy** al publicarse y la limpieza (GC) es semanal.

Despliegues Docker

El agente **rescue-agent**, escrito en Rust y conectado con **TLS mutuo**, gestiona stacks Compose, builds y procedimientos. Envía alertas de salud y muestra los logs en vivo.

GitOps a Kubernetes

Soporta Helm, Kustomize y YAML. El diff y el apply se hacen del lado del servidor, con *prune*, *self-heal* y reconciliación cada 3 minutos. **La sincronización se bloquea si la imagen tiene vulnerabilidades críticas.**

Clústeres detrás de NAT

El agente abre un túnel saliente, así que gestionas clústeres en la red del cliente sin abrir puertos de entrada. Los AppProjects separan equipos y entornos.

EXPLORADOR KUBERNETES NATIVO

- Recursos y **topología**
- Detección de **problemas**
- 40 **comprobaciones**
- Terminal **auditada**
- Línea de **tiempo**
- Helm con **rollback**
- Capacidad y **costo**
- Mapa de **tráfico**
- Logs en **vivo**

ISO/IEC 27001:2022

EVIDENCIA QUE SE VERIFICA SOLA

Cada evento de seguridad queda en un registro **append-only**, encadenado por hash y firmado con **Ed25519** (RFC 8032). El mapa de cobertura muestra el estado de cada control, y los paquetes de evidencia en **PDF**, **XLSX** y **JSON** pueden verificarse fuera de la plataforma, sin depender de ella.

A.5.7	Inteligencia de amenazas	Fuentes CISA KEV, EPSS y OSV en la priorización.
A.8.8	Gestión de vulnerabilidades técnicas	Hallazgos deduplicados, SLA por severidad y aceptación de riesgo.
A.8.9	Gestión de la configuración	Ramas protegidas y GitOps declarativo con self-heal.
A.8.19	Instalación de software	Despliegues solo vía pipeline, agente mTLS y GitOps.
A.8.25	Ciclo de vida de desarrollo seguro	Pipeline DevSecOps en cada cambio.
A.8.26	Requisitos de seguridad de aplicaciones	Gate de seguridad obligatorio en los pull requests.
A.8.27	Arquitectura e ingeniería segura	Aprovisionamiento con el perfil devsecops-standard.
A.8.28	Codificación segura	AI-SAST con reglas CWE/OWASP y detección de secretos.
A.8.29	Pruebas de seguridad	Escaneo en CI y en el registro antes de producción.
A.8.30	Desarrollo externalizado	Terceros trabajan por fork + PR, bajo los mismos controles.
A.8.31	Separación de entornos	Ramas develop, QA y main con promoción controlada.
A.8.32	Gestión de cambios	Revisión, checks y trazabilidad de cada merge.

FICHA TÉCNICA

ESPECIFICACIONES

Arquitectura	Aplicación web renderizada en servidor (sin SPA), multi-cliente con aislamiento verificado por pruebas automáticas.
Backend	Python 3.12 · Django 5.1 · Django REST Framework con OpenAPI · Celery 5.4 (worker y beat)
Datos	PostgreSQL 16 · Redis 7 (caché, sesiones y colas) · almacenamiento de objetos S3 / MinIO
Interfaz	HTMX · Alpine.js · Tailwind CSS · gráficas Chart.js · modo oscuro · español (Colombia)
Despliegue	Docker Compose con proxy Caddy, servidor Git, runner CI, workers, registro y servicios de observación de Kubernetes
Agente remoto	rescue-agent en Rust (tokio, rustls) con TLS mutuo y túnel saliente
Herramientas incluidas	kubectrl · Helm · Kustomize · Trivy · Gitleaks · cdxgen
Estándares	ISO/IEC 27001:2022 · CWE · OWASP · CVSS 3.1 · SARIF 2.1.0 · CycloneDX 1.6 · VEX · CISA KEV · EPSS · OSV
Autenticación	Contraseñas con Argon2 · 2FA TOTP · LDAP / Active Directory por cliente
Autorización	RBAC con 6 roles (admin, secops, developer, auditor, viewer, system) y permisos por objeto
Protección de datos	Secretos cifrados (Fernet) · HTTPS / HSTS · límite de peticiones · nada se borra definitivamente: eventos y evidencia append-only
APIs	REST nativa · API compatible con Gitea /api/v1 · API de diagnóstico de solo lectura con claves con caducidad y restricción por IP

TU CÓDIGO SEGURO, NUESTRA PRIORIDAD



T.I RESCUE
SEGURIDAD INFORMÁTICA

CONTÁCTANOS

Agenda una demostración de Rescue DevSecOps o conversa con nuestro equipo sobre cómo llevar tu desarrollo al cumplimiento de ISO 27001.

- Cra. 65 #8B-91 Ofic. 485, Guayabal, Medellín, Antioquia • WhatsApp: +57 315 893 7873
- Teléfono fijo: +57 4 6073303 • info@tirescue.com.co • www.tirescue.com

WWW.TIRESCUE.COM
Expertos en ciberseguridad