José Alvarado Mazzei

Full Stack Developer & Infrastructure Engineer

Temuco, Chile (Remoto) · +56 9 4893 7755 · jose@alvaradomazzei.cl · alvaradomazzei.cl · linkedin.com/in/josealvaradomazzeies

PERFIL PROFESIONAL

Desarrollador Full Stack semi-senior (3+ años, Laravel/PHP + Vue.js) en transición hacia DevSecOps, cursando Ingeniería en Ciberseguridad (INACAP). Combino experiencia real en CI/CD (GitHub Actions con SCA, secret scanning y deploy automatizado), administración de infraestructura Linux en producción (8 VPS, hardening, respaldos cifrados) y prácticas de seguridad aplicada: análisis de vulnerabilidades con OpenVAS/Greenbone, gestión segura de secretos, defensa en profundidad y cumplimiento normativo. Mantengo proyectos públicos verificables que demuestran la integración de seguridad en el SDLC y arquitectura cloud segura en AWS. Lideré la certificación de una plataforma de control de asistencia ante la Dirección del Trabajo de Chile (Resolución 38 Exenta).

HABILIDADES TÉCNICAS

Seguridad & DevSecOps: Defensa en profundidad, análisis SCA (composer audit, pnpm audit, Dependabot), secret scanning (gitleaks), análisis de vulnerabilidades (OpenVAS/Greenbone), hardening Linux, security headers (HSTS/CSP), hashing SHA-256, gestión de secretos server-side, cumplimiento normativo (Resolución 38 Exenta)

CI/CD & Automatización: GitHub Actions (pipelines multi-job: quality, security, secrets, deploy), Laravel Pint, PHPUnit, deploy automatizado por SSH, scripting Bash/Python, Git (branching, PRs, code review)

Cloud (AWS) hands-on: VPC, EC2, RDS, Security Groups encadenados, IP elástica, KMS, patrón Bastion Host, arquitectura híbrida On-Premise/On-Cloud

Contenedores & Linux: Docker / Docker Compose (entornos dev/prod multi-container en producción), Nginx, WireGuard VPN, Ubuntu 22.04/24.04, observabilidad (Nginx → Vector → Postgres → Superset)

Backend & APIs: Laravel 10/11/13, PHP 8.2–8.4, APIs RESTful, integración de sistemas, Node.js

Bases de Datos: MySQL 8.0 (replicación Master-Slave geográfica con failover), MariaDB, PostgreSQL, Redis

EXPERIENCIA PROFESIONAL

Encargado de Área Informática / Tech Lead — Energiza SPA — Remoto

Enero 2025 – Presente

- Responsable único de toda la infraestructura tecnológica y continuidad operativa de la empresa tras la reducción del equipo.
- Administración de 8 VPS en producción (Contabo) distribuidos en 3 regiones geográficas: ~40 vCPUs, ~106 GB RAM y ~3.4 TB de almacenamiento, más ~1.25 TB en Object Storage S3.
- Lideré la solicitud y documentación técnica de certificación del sistema Vanadio ante la Dirección del Trabajo de Chile (Resolución 38 Exenta), cubriendo enrolamiento e identificación, integridad criptográfica de marcaciones, transmisión segura, disponibilidad/replicación y seguridad general (Art. 14).
- Implementé análisis de vulnerabilidades con OpenVAS/Greenbone en producción (escaneos Full and Fast, gestión de hallazgos y overrides de falsos positivos justificados); resultado: 0 vulnerabilidades Critical/High/Medium/Low en el host principal de Vanadio.
- Hardening del SDLC: security headers (HSTS/CSP), gestión de secretos por variables de entorno, integridad de registros mediante hash SHA-256, control de acceso por roles (Spatie), fail2ban y firewall.
- Operación de servidores con 60+ días de uptime continuo sin incidentes; stack Linux con Nginx, Docker, MySQL/MariaDB, Redis y PHP 8.2–8.4.
- Migración completa de hosting compartido a VPS dedicado: infraestructura, 178 buzones de correo, 2 plataformas Moodle (upgrade 3.11 → 5.0) y DNS autoritativo propio.
- Estrategia de respaldos en 3 capas (hypervisor + Object Storage S3 + off-site) con cifrado GPG AES-256.
- Pipeline de telemetría propio (Nginx → Vector → Postgres → Superset) con dashboards de tráfico en tiempo real.

Desarrollador Full Stack — Energiza SPA — Remoto

Enero 2023 – Enero 2025

- Desarrollo de aplicaciones empresariales en Laravel para control de asistencia, permisos, delegación de roles y reportería laboral.
- Implementación de APIs REST para sincronización de dispositivos biométricos con bases de datos empresariales.
- Integración nativa de lectores de huella HID DigitalPersona mediante SDK en C# .NET.
- Desarrollo de dashboards administrativos y herramientas de gestión multi-empresa.
- Despliegue de aplicaciones en infraestructura Linux/cloud y administración de repositorios Git en equipo distribuido.

PRÁCTICAS DEVSECOPS IMPLEMENTADAS

- CI/CD con seguridad integrada: pipelines GitHub Actions multi-job (lint, tests, SCA, secret scanning, deploy) en proyectos propios.
- SCA (Software Composition Analysis): composer audit y pnpm audit en cada build; remediación real de CVEs (no supresión), por ejemplo 3 CVEs de Symfony resueltos vía composer update sin romper la suite de tests.
- Secret scanning con gitleaks sobre código e historial completo del repositorio.
- Gestión de secretos: plantillas .env.example versionadas, secretos generados server-side con openssl rand, cifrado age en backups, Vaultwarden como gestor centralizado, GitHub Secrets para credenciales de CI/CD.
- Shift-left: pre-commit hook propio que bloquea commits con secretos en staging.
- Red y transporte: SSH ed25519 en puerto no estándar, TLS automático con HSTS preload, malla WireGuard autoadministrada.
- Contenedores: Docker Compose dev/prod con paridad de entornos, sin exponer puertos de BD en producción, datos y secretos fuera de la imagen.
- Defensa anti supply-chain: pnpm con --frozen-lockfile y --ignore-scripts.
- Backups y DR: respaldos automatizados cifrados con age, retención por ciclos, restore documentado y probado.
- Análisis de vulnerabilidades de infraestructura con OpenVAS/Greenbone, gestión de hallazgos y overrides justificados.
- Documentación de seguridad: SECURITY.md por proyecto, runbooks operativos, audit log append-only de decisiones.

PROYECTOS PÚBLICOS

Crono — Pipeline CI/CD con seguridad integrada

github.com/c0hete/CronoApp

- SaaS de control de asistencia (Laravel 13 + PWA + Docker) en producción, con pipeline GitHub Actions de 4 jobs: quality (Laravel Pint + 69 tests PHPUnit), security/SCA (composer audit + pnpm audit), secrets (gitleaks sobre historial completo) y deploy automatizado vía SSH a contenedores Docker.
- Resultado verificable: detecté y remedié 3 CVEs reales de Symfony en el primer run, vía composer update sin romper los 69 tests (criterio aplicado: detectar ≠ ignorar).
- Credenciales fuera del repo (host, puerto, usuario y llave como GitHub Secrets); SECURITY.md con política de remediación e interpretación de resultados.

Olympo — Arquitectura segura On-Premise / On-Cloud en AWS

github.com/c0hete/proyecto-olympo

- Arquitectura híbrida que conecta un servidor local con una base de datos privada en AWS aplicando patrón Bastion Host: VPC dedicada, EC2 con IP elástica, RDS MySQL en subred privada sin ruta a internet, Security Groups encadenados, KMS para cifrado en reposo, túnel SSH cifrado, cliente CRUD en Python.
- Defensa en profundidad de 3 capas: topología (RDS inalcanzable por estructura, no solo por firewall), Security Groups encadenados (identidad a nivel de recurso) y autenticación SSH por llave.
- Least privilege aplicado: SSH solo desde IPs autorizadas, auth por contraseña desactivada, datos AWS reales anonimizados antes de publicar; CI propio (ruff + gitleaks); diseño documentado para migrar a AWS Secrets Manager con rotación automática.

PROYECTO DESTACADO

Sistema Vanadio — Plataforma SaaS de Control de Asistencia Biométrico

Rol: Diseño de arquitectura, desarrollo full stack e infraestructura.

- Plataforma multi-tenant que da servicio a múltiples empresas, en cumplimiento con la Resolución 38 Exenta de la Dirección del Trabajo de Chile.

- Alta disponibilidad geográfica: replicación MySQL Master-Slave entre servidores en EE.UU. y Europa sobre VPN WireGuard, con failover automatizado vía GitHub Actions + Cloudflare API.
- Integración de hardware biométrico (HID DigitalPersona 4500U) mediante API puente en C# .NET 8.
- Integridad de registros mediante hash criptográfico, control de acceso por roles (Spatie) y respaldos externos cifrados (Backblaze B2 + GPG).
- PWA con sincronización offline para marcaje móvil conforme al Art. 10 de la Resolución 38.

EDUCACIÓN

Ingeniería en Ciberseguridad — INACAP (en curso, alumno regular 2026)
Técnico de Nivel Superior Analista Programador — INACAP (titulado enero 2026). Ranking de egreso: 4° de 71. Nota 6.4/7.0.

CERTIFICACIONES

- Claude Code in Action — Anthropic (2025)
- Infraestructura TI Segura — INACAP (144h: Sistemas Operativos, Seguridad de la Información)
- Desarrollador Full Stack — INACAP (144h: Front End, Back End)
- Desarrollo de Aplicaciones Iniciales — INACAP (162h: Programación Segura, POO Segura)

Experiencia práctica con AWS (VPC, EC2, RDS, Security Groups) mediante proyectos académicos y tareas en producción.

IDIOMAS

Español — Nativo
Inglés — Lectura y comprensión técnica avanzada; conversacional intermedio

N°13923349

CERTIFICADO ALUMNO

El INSTITUTO PROFESIONAL INACAP, certifica que Jose Rafael Alvarado Mazzei Cédula de Identidad N° 25.768.863-1 , es alumno regular en la jornada Diurna del Programa de Estudio Ingeniería en Ciberseguridad, conducente al Título Profesional Ingeniero en Ciberseguridad, cuya duración es de 8 semestres.

Vigencia: durante el Primer Semestre Académico del año 2026.

Se extiende el presente Certificado a solicitud del interesado para los fines que estime convenientes.

Temuco, 25 de Mayo de 2026

CÓDIGO DE VERIFICACIÓN
8D2EC12D81FCEF7C

Fecha de Emisión 25-05-2026 22:33:44 hrs. - Incorpora Firma Electrónica Avanzada
La Institución o persona ante quien se presente este Certificado, podrá verificarlo en www.inacap.cl

INSTITUTO PROFESIONAL INACAP SECRETARIA GENERAL

MARIA SOLEDAD FIGUEROA MANDIOLA
SECRETARIA GENERAL

N°13440992

CERTIFICADO EN INFRAESTRUCTURA TI SEGURA

CENTRO DE FORMACIÓN TÉCNICA INACAP RUT Nº 87.020.800-6,
Certifica que Jose Rafael Alvarado Mazzei Rut: 25.768.863-1 ha
obtenido el certificado en **INFRAESTRUCTURA TI SEGURA**,
con una duración total de 144 horas.

Entregado el 16 de enero de 2026

CÓDIGO DE VERIFICACIÓN
2D97B768C3831BBC

Fecha de Emisión 16-01-2026 13:15:59 hrs. - Incorpora Firma Electrónica Avanzada
La Institución o persona ante quien se presente este Certificado, podrá verificarlo en www.inacap.cl

INSTITUTO PROFESIONAL
SECRETARIA GENERAL
INACAP

MARIA SOLEDAD FIGUEROA MANDIOLA
SECRETARIA GENERAL

El presente certificado corresponde a las siguientes asignaturas:

* Fundamentos de Seguridad de la Información, 72 horas.
* Sistemas Operativos, 72 horas.

Header Place Holder

Sign Place Holder

N°13442056

CERTIFICADO DE TITULO

(COPIA)

Certifico que con fecha 16 de Enero de 2026

Jose Rafael Alvarado Mazzei

Rut: 25.768.863-1

cumplió con los requisitos exigidos por El CENTRO DE FORMACIÓN TÉCNICA INACAP

y ha obtenido el Título

Técnico de Nivel Superior Analista Programador

Número 7.536.649 del Registro General de Títulos y Certificados de esta Institución.

Santiago, 16 de Enero de 2026

CÓDIGO DE VERIFICACIÓN
65AC7C43CC7A5C0E

Fecha de Emisión 16-01-2026 15:46:39 hrs. - Incorpora Firma Electrónica Avanzada
La Institución o persona ante quien se presente este Certificado, podrá verificarlo en www.inacap.cl

INSTITUTO PROFESIONAL SECRETARIA GENERAL INACAP

MARIA SOLEDAD FIGUEROA MANDIOLA
SECRETARIA GENERAL

RESERVADO CABECERA FIRMA DIGITAL

RESERVADO PARA FIRMA ELECTRONICA - SIGN

CERTIFICATE of COMPLETION

JOSE ALVARADO MAZZEI

has completed

Claude Code in Action

Issued: Dec. 14, 2025
Certificate No: c62icwiaq936
View: https://verify.skilljar.com/c/c62icwiaq936

ANTHROP\C