🇪🇸 Versión en Español

Mejores Prácticas de Seguridad para Ingenieros de Software

La **seguridad del software** es un elemento crítico para proteger sistemas, datos y la confianza de los clientes. En NetGuard Solutions, sabemos que los ingenieros de software juegan un rol clave en prevenir vulnerabilidades y garantizar despliegues seguros.

🔑 1. Gestión de Credenciales Seguras

- **No incluir claves o contraseñas en el código.**
- Usar **variables de entorno** o gestores de secretos como **HashiCorp Vault** o **AWS Secrets Manager**.
- Rotar credenciales regularmente y aplicar el principio de **mínimos privilegios**.

> 💡 Tip: Los archivos `.env` deben usarse solo localmente y nunca subirse a repositorios públicos.

✅ 2. Revisiones de Código y Análisis de Seguridad

- Realizar revisiones de pares centradas en vulnerabilidades de red y software.
- Seguir el **OWASP Top 10** para prevenir fallos comunes.
- Integrar herramientas de análisis estático: **SonarQube**, **ESLint (reglas de seguridad)**.
- Asegurarse de: validación de entradas, manejo correcto de errores y registros seguros.

🛠️ 3. Seguridad de la Cadena de Suministro

- Gestionar dependencias con cuidado y actualizar librerías vulnerables.
- Escanear dependencias con **Snyk**, **Dependabot** o `npm audit`.
- Mantener un registro interno de librerías aprobadas para mayor control.

🚀 4. Protección del Pipeline CI/CD

- Incluir **puertas de seguridad**: linting, pruebas unitarias, escaneo de vulnerabilidades.
- Limitar acceso de escritura a ramas principales y exigir aprobaciones manuales.
- Firmar artefactos y verificar integridad antes de despliegues en producción.

> 📊 Según **Veracode**, el 70% de las vulnerabilidades se detectan en el ciclo de desarrollo. Mitigarlas temprano reduce riesgos y costos.

🌐 Con NetGuard Solutions

Nuestras soluciones ayudan a empresas en **finanzas, salud, tecnología y telecomunicaciones** a integrar seguridad desde el desarrollo hasta la operación. Con estas prácticas, los ingenieros de software protegen aplicaciones, datos y la confianza de los clientes.

> 🔹 Seguridad + Desarrollo = Software confiable y robusto

🇬🇧 English Version

Security Best Practices for Software Engineers

Software security is a critical component for protecting systems, data, and client trust. At NetGuard Solutions, we understand that software engineers play a key role in preventing vulnerabilities and ensuring secure deployments.

🔑 1. Secure Credentials Management

- **Never include keys or passwords in code.**
- Use **environment variables** or secret managers such as **HashiCorp Vault** or **AWS Secrets Manager**.
- Rotate credentials regularly and apply the **principle of least privilege**.

> 💡 Tip: `.env` files should be used only locally and never committed to public repositories.

✅ 2. Code Reviews and Security Analysis

- Conduct peer reviews focused on network and software vulnerabilities.
- Follow the **OWASP Top 10** to prevent common security issues.
- Integrate static analysis tools like **SonarQube** or **ESLint security rules**.
- Ensure input validation, proper error handling, and secure logging.

🛠️ 3. Supply Chain Security

- Carefully manage dependencies and promptly update vulnerable libraries.
- Scan dependencies with **Snyk**, **Dependabot**, or `npm audit`.
- Maintain an internal registry of approved libraries for better control.

🚀 4. CI/CD Pipeline Protection

- Implement **security gates**: linting, unit testing, vulnerability scanning.
- Restrict write access to main branches and require manual approvals.
- Sign artifacts and verify integrity before production deployment.

> 📊 According to **Veracode**, 70% of vulnerabilities are found during the development cycle. Mitigating them early reduces both risk and cost.

🌐 With NetGuard Solutions

Our solutions help companies in **finance, healthcare, technology, and telecommunications** integrate security from development through operations. By following these best practices, software engineers protect applications, data, and client trust.

> 🔹 Security + Development = Reliable, robust software

Guía Oficial de Instalación y Uso 📘 Para Administradores, Desarrolladores y Colaboradores

NetGuard Pro está diseñado para un despliegue rápido y seguro. Sigue los pasos a continuación para instalar y configurar la plataforma en tu entorno empresarial.

📌 Características Principales 🔧 Optimización de Red

- Monitoreo automatizado del rendimiento.
- Asignación dinámica de ancho de banda.
- Análisis en tiempo real de calidad y disponibilidad.

🛡️ Seguridad Mejorada

- Gestión de firewall integrada.
- Detección inteligente de amenazas.
- Transmisión de datos cifrada con TLS 1.3.

📈 Escalabilidad

- Soporte para scaling horizontal sin interrupciones.
- Integración con AWS, Azure y GCP.
- Balanceo automático de carga.

🖥️ Interfaz Intuitiva

- Panel personalizable según rol.
- Vistas dinámicas y métricas avanzadas.
- API para automatización de procesos.

🖥️ Requisitos del Sistema
Sistema Operativo:

- Windows Server 2016/2019
- Ubuntu 20.04+
- CentOS 7+
- macOS 10.15+

Procesador:

- Mínimo: Quad-core 2.5 GHz
- Recomendado: Octa-core 3.0 GHz

Memoria RAM:

- Mínimo: 8 GB
- Recomendado: 16 GB

Almacenamiento:

- Mínimo: 500 GB
- Recomendado: 1 TB SSD

Red:

- Mínimo: 1 Gbps
- Recomendado: 10 Gbps

🔌 Integraciones Compatibles
Proveedores de Nube:

- AWS
- Azure
- GCP

🔌Herramientas de Terceros:

- Slack
- PagerDuty
- Splunk

💼 Licenciamiento y Precios

- Pequeñas Empresas: Hasta 5 servidores — $499/mes
- Empresas Medianas: Hasta 15 servidores — $1,299/mes
- Corporativo / Enterprise: Más de 15 servidores — Precio personalizado

🚀 Guía Rápida de Instalación
1️⃣Descarga e Instalación
Descarga desde el portal oficial .
Ejecuta el instalador para tu sistema operativo.

2️⃣Configuración Inicial
Configura manualmente o importa .json / .yaml.
Define credenciales iniciales del administrador.

3️⃣Activación de Licencia
Ingresa la clave asignada o activa la prueba de 30 días.

4️⃣Integración de Red
Usa detección automática de topologías.
Conecta segmentos, gateways y dispositivos clave.

5️⃣Panel de Control
Personaliza widgets y vistas por rol.
Activa métricas avanzadas para monitoreo continuo.

📚 Ejemplo de Caso de Uso
Empresa XYZ:
Optimiza ancho de banda según carga de trabajo.
Bloquea los intentos de acceso no autorizados en tiempo real.

Genera reportes diarios sobre rendimiento de la red.

✅ Resultado: mayor eficiencia, seguridad y visibilidad completa.

🛠️ Para Desarrolladores y Colaboradores

Estructura del Proyecto: Backend modular con API RESTful, almacenamiento seguro y panel web.

Contribuciones: Siga los estándares de codificación y flujo de Pull Requests.
Pruebas: Ejecute pruebas unitarias e integradas antes de enviar cambios.

📑 Notas Finales

Este README es una guía rápida para un despliegue estándar y seguro de NetGuard Pro. Para configuraciones avanzadas (HA, gateways dedicados, automatización API, exportación SIEM), consulte la documentación extendida o contacte al representante técnico.