Archivo de Configuración de Variables de Entorno (.env)

Configuración Completa del Sistema IoT

Descripción General

Este archivo .env contiene todas las variables de configuración necesarias para el funcionamiento del ecosistema IoT, organizadas en secciones lógicas que permiten una gestión centralizada y segura de la configuración.

🚀 Configuración del Servidor Node.js

Entorno de Ejecución

env

NODE_ENV=development
PORT=4000

NODE_ENV: Ambiente de desarrollo con herramientas de debugging

PORT: Puerto 4000 para el servidor backend (diferente al default 3000)

Modo Desarrollo

env

DEV_MODE=true
DEV_USER_EMAIL=admin@localhost.com
DEV_USER_NAME=Administrador Local

DEV_MODE: Habilita autenticación simplificada sin Google OAuth

Credenciales de desarrollo: Usuario por defecto para testing

☁️ Configuración Cloudflare Tunnel

Token de Túnel

env

CLOUDFLARE_TUNNEL_TOKEN=eyJhIjoiYzk3ZDU0ZjhiNzQyNWUwM2VkM2YzODk3YjlmNGJlODIiLCJ0IjoiZmVjMTIzNmQtYTJkOS00MTU5LTgzOWYtMDE5MDk2MjI5OTFkIiwicyI6Ik4yWTJOakk0TWpndE1UWmlPU>

Túnel seguro: Exposición de servicios sin abrir puertos

Token embebido: Autenticación con Cloudflare

Comentado alternativo: Opción para configuración personalizada

🔐 Sistema de Autenticación JWT

Configuración de Tokens

env

JWT_SECRET=2fe600301bc1e4e129c5519d32bed987cb521c3281b5e40027e37fee64a
bd7ae706f56388a8f1c507889b09b9ef1de3822f232bc798b03680f7bb943849910fc
JWT_EXPIRES_IN=15m
REFRESH_EXPIRES_IN=7d

Clave segura: 64 bytes hexadecimales generados criptográficamente

Expiración corta: 15 minutos para tokens de acceso

Refresh largo: 7 días para tokens de renovación

🔗 Integración Google OAuth2

Identidad de Google

env

GOOGLE_CLIENT_ID=113014965393-
9t3h4eg2jr4aj7mfs4q78kkajln16m79.apps.googleusercontent.com

Client ID: Identificador de aplicación en Google Cloud Console

OAuth2: Autenticación social para usuarios

🌐 Configuración CORS

Orígenes Permitidos

env

CORS_ORIGIN=http://127.0.0.1:8080,http://localhost:8080,https://iot-
opalo.work,http://app.ispciot.org

Desarrollo local: localhost en puerto 8080

Producción: Dominios públicos de la aplicación

HTTP/HTTPS: Mezcla para transición a SSL

👥 Sistema de Roles y Autorización

Listas de Control de Acceso

env

ADMIN_WHITELIST=vittodutti@gmail.com
ACTION_WHITELIST=

Administradores: Usuario con acceso completo al sistema

Acción: Lista vacía para permisos intermedios

Formato: Emails separados por comas

📡 Configuración MQTT para IoT

Broker MQTT

env

MQTT_BROKER_HOST=mqtt.ispciot.org
MQTT_BROKER_PORT=80
MQTT_BROKER_USERNAME=
MQTT_BROKER_PASSWORD=
MQTT_TOPICS=sensors/temperature,sensors/humidity

Host público: Broker accesible externamente

Puerto 80: Para evitar bloqueos de firewall

Topics: Sensores de temperatura y humedad por defecto

🗄️ Configuración de Bases de Datos

MariaDB/MySQL

env

MYSQL_HOST=172.18.0.4
MYSQL_ROOT_PASSWORD=root@siloiot2025
MYSQL_DATABASE=silo_db
MYSQL_USER=silo_user
MYSQL_PASSWORD=user@siloiot2015

IP estática: 172.18.0.4 en red Docker

Credenciales seguras: Contraseñas complejas

Usuario dedicado: silo_user con permisos específicos

InfluxDB para Series Temporales

env

INFLUXDB_DB=metricas_silo
INFLUXDB_ADMIN_USER=admin
INFLUXDB_ADMIN_PASSWORD=influx@siloiot2025

INFLUXDB_USER=telegraf_user
INFLUXDB_USER_PASSWORD=telegraf@siloiot2025

Base de métricas: Almacenamiento de datos de sensores

Dos usuarios: Admin y usuario de Telegraf separados

Contraseñas específicas: Seguridad por rol

📊 Sistema de Visualización Grafana

Acceso Administrativo

env

GRAFANA_ADMIN_USER=admin
GRAFANA_ADMIN_PASSWORD=grafana@siloiot2025

Credenciales default: Usuario admin con contraseña segura

Dashboards: Para visualización de métricas IoT

💾 Configuración de Backup

Políticas de Respaldo

env

BACKUP_ENABLED=true
BACKUP_SCHEDULE=0 2 * * *
BACKUP_RETENTION_DAYS=30
BACKUP_PATH=/backups

Automático: Activado para respaldos regulares

Horario: 2:00 AM diariamente (formato cron)

Retención: 30 días de backups históricos

📧 Sistema de Notificaciones

Configuración SMTP

env

SMTP_HOST=smtp.gmail.com
SMTP_PORT=587
SMTP_USER=notifications@tudominio.com
SMTP_PASS=your-smtp-password

Gmail SMTP: Servidor de correo saliente

Puerto TLS: 587 para conexiones seguras

Cuenta dedicada: Para notificaciones del sistema

Webhooks para Integraciones

env

WEBHOOK_URL=https://hooks.slack.com/services/YOUR/SLACK/WEBHOOK

Slack: Integración para notificaciones en tiempo real

Placeholder: URL a reemplazar con configuración real

📈 Sistema de Monitoreo

Configuración de Logs

env

LOG_LEVEL=info
LOG_FILE=/var/log/iot-app.log

Nivel info: Balance entre detalle y rendimiento

Archivo centralizado: Todos los logs en ubicación específica

Métricas del Sistema

env

METRICS_ENABLED=true
METRICS_PORT=9090

Métricas activadas: Recolección de datos de performance

Puerto específico: 9090 para scraping de métricas

🌍 Configuración de Producción

Dominios y SSL

env

DOMAIN=app.ispciot.org
SSL_EMAIL=vittodutti@gmail.com

Dominio principal: app.ispciot.org para acceso público

Email SSL: Para certificados Let's Encrypt

Reverse Proxy

env

REVERSE_PROXY_HOST=nginx-proxy-manager
REVERSE_PROXY_PORT=80

Proxy manager: Servicio centralizado de reverse proxy

Puerto interno: 80 para comunicación entre contenedores

🔒 Consideraciones de Seguridad

Variables Críticas

JWT_SECRET: Debe ser único por ambiente y mantenerse secreto

Contraseñas de BD: Diferentes para cada usuario y servicio

Tokens externos: Cloudflare token debe protegerse

Configuración por Ambiente

Desarrollo: DEV_MODE=true, logs detallados

Producción: DEV_MODE=false, configuración optimizada

🛠️ Notas de Implementación

Valores por Defecto vs Personalizados

Topics MQTT: Configuración básica para empezar

Credenciales: Placeholders para reemplazar con valores reales

IPs de red: Específicas del despliegue Docker

Variables Opcionales vs Requeridas

Cloudflare: Opcional para exposición pública

Notificaciones: Configurables según necesidades

Backup: Activado por defecto para protección de datos

Esta configuración proporciona una base completa para el sistema IoT, permitiendo fácil adaptación entre ambientes mientras mantiene estándares de seguridad apropiados.