Configuración de Variables de Entorno

Archivo de Configuración del Sistema (.env)

Descripción General

Este archivo .env contiene todas las variables de configuración necesarias para el funcionamiento del sistema IoT, organizadas en secciones lógicas que cubren desde el entorno de ejecución hasta integraciones con servicios externos y configuraciones de producción.

Configuración del Servidor Node.js

Entorno de Ejecución

env

NODE_ENV=development
PORT=3000

NODE_ENV: Define el ambiente como desarrollo, activando herramientas de debugging y logs detallados

PORT: Puerto donde el servidor backend escuchará las conexiones (3000)

Modo Desarrollo

env

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

DEV_MODE: Habilita autenticación simplificada para desarrollo

DEV_USER_EMAIL: Email del usuario de desarrollo por defecto

DEV_USER_NAME: Nombre mostrado para el usuario de desarrollo

Sistema de Autenticación JWT

Configuración de Tokens

env

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

JWT_SECRET: Clave criptográfica de 64 bytes para firmar tokens (generada seguramente)

JWT_EXPIRES_IN: Expiración de tokens de acceso (15 minutos para seguridad)

REFRESH_EXPIRES_IN: Expiración de tokens de refresco (7 días)

Integración con Google Identity

OAuth2 Configuration

env

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

GOOGLE_CLIENT_ID: Identificador de la aplicación en Google Cloud Console para autenticación OAuth2

Configuración CORS (Cross-Origin Resource Sharing)

Orígenes Permitidos

env

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

Desarrollo local: localhost y 127.0.0.1 en puerto 8080

Producción: Dominios públicos de la aplicación

Seguridad: Lista explícita de orígenes permitidos

Sistema de Roles y Autorización

Listas de Control de Acceso

env

ADMIN_WHITELIST=vittodutti@gmail.com
ACTION_WHITELIST=

ADMIN_WHITELIST: Usuarios con rol de administrador (acceso completo)

ACTION_WHITELIST: Usuarios con permisos de acción (operaciones específicas)

Formato: Lista separada por comas, emails en minúsculas

Configuración MQTT para Comunicación IoT

Broker MQTT

env

```
MQTT_BROKER_HOST=mqtt.ispciot.org
MQTT_BROKER_PORT=80
MQTT_BROKER_USERNAME=
MQTT_BROKER_PASSWORD=
```

Host: Servidor MQTT público accesible

Puerto: 80 para compatibilidad con restricciones de red

Autenticación: Credenciales vacías para conexión anónima

Configuración de Bases de Datos

MariaDB/MySQL

env

```
MYSQL_HOST=172.18.0.2
MYSQL_ROOT_PASSWORD=root@siloiot2025
MYSQL_DATABASE=silo_db
MYSQL_USER=silo_user
MYSQL_PASSWORD=user@siloiot2015
```

Host: IP del contenedor de base de datos en red Docker

Credenciales: Contraseñas seguras para root y usuario de aplicación

Base de datos: Nomme de la base de datos principal

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 datos: Almacenamiento para métricas de sensores

Usuarios: Separación entre administrador y usuario de aplicación

Contraseñas: Credenciales seguras específicas por rol

Sistema de Visualización Grafana

Acceso Administrativo

env

```
GRAFANA_ADMIN_USER=admin
GRAFANA_ADMIN_PASSWORD=grafana@siloiot2025
```

Usuario: Credenciales para acceso al panel de Grafana

Contraseña: Clave segura para cuenta administrativa

Configuración de Backup Automático

Políticas de Respaldo

env

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

Habilitado: Sistema de backup activo

Horario: Ejecución diaria a las 2:00 AM (formato cron)

Retención: Conservación de backups por 30 días

Ruta: Directorio de almacenamiento de backups

Sistema de Notificaciones

Configuración SMTP para Email

env

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

Servidor: Gmail como proveedor SMTP

Puerto: 587 para TLS

Credenciales: Cuenta dedicada para notificaciones

Webhooks para Integraciones

env

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

Slack: URL para enviar notificaciones a canales de Slack

Extensible: Puede configurarse para otros servicios

Sistema de Monitoreo y Logs

Configuración de Logging

env

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

Nivel: Info para balance entre detalle y rendimiento

Archivo: Ruta centralizada para logs de aplicación

Métricas del Sistema

env

METRICS_ENABLED=true
METRICS_PORT=9090

Habilitado: Recolección de métricas activa

Puerto: Endpoint para scraping de métricas

Configuración de Producción

Dominio y SSL

env

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

Dominio: URL pública de la aplicación

Email SSL: Contacto para certificados Let's Encrypt

Reverse Proxy

env

REVERSE_PROXY_HOST=nginx-proxy-manager
REVERSE_PROXY_PORT=80

Host: Nombre del servicio de proxy en Docker

Puerto: Puerto interno del proxy

Consideraciones de Seguridad

Manejo de Secretos

Variables críticas: JWT_SECRET y contraseñas deben ser únicas por ambiente

Exclusión: Archivo .env debe estar en .gitignore

Rotación: Contraseñas deben rotarse periódicamente

Configuración por Ambiente

Desarrollo: DEV_MODE=true, logs detallados

Producción: DEV_MODE=false, configuración optimizada

Variables Dependientes del Contexto

Red Docker

MYSQL_HOST: IP específica del contenedor de base de datos

REVERSE_PROXY_HOST: Nombre del servicio en docker-compose

Servicios Externos

GOOGLE_CLIENT_ID: Configurado en Google Cloud Console

SMTP_*: Dependiente del proveedor de email

WEBHOOK_URL: Específico del servicio de mensajería

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