

Seguridad y Cumplimiento

Cómo Oracle Health Dashboard protege tus credenciales, tus datos y tu licencia. Diseñado para entornos corporativos exigentes y auditorías.

On-premise

Sin telemetría

Cifrado en reposo

CAPÍTULO

01 - Principios de diseño

La seguridad no es un añadido: guía cada decisión del producto.

- › **Mínimo privilegio** : opera con un usuario Oracle de solo lectura.
- › **On-premise** : corre íntegramente en tu infraestructura; **sin telemetría** ni llamadas externas.
- › **Cifrado en reposo** para credenciales y secretos.
- › **Sin paquetes licenciados** de Oracle: solo vistas base (cumplimiento).
- › **Defensa en profundidad** : autenticación, anti fuerza bruta, endurecimiento de cookies.

CAPÍTULO

02 - Acceso a la base de datos

El dashboard nunca modifica tus bases ni usa funciones licenciadas.

- › Requiere solo **CREATE SESSION** + **SELECT_CATALOG_ROLE** (solo lectura).
- › Usa exclusivamente **vistas base** (V\$/DBA_): **no** usa Diagnostic ni Tuning Pack.
- › Conexión en modo **thin** : sin Oracle Client que parchear o mantener.

› Las consultas son estáticas y parametrizadas: **sin superficie de SQL injection** .

! “Solo vistas base” es además un control de **cumplimiento**: evita el uso accidental de funciones que requieren licencias adicionales de Oracle.

CAPÍTULO

03 - Protección de credenciales

Las contraseñas de tus bases se guardan cifradas y ligadas al equipo.

ASPECTO	IMPLEMENTACIÓN
Cifrado	Fernet (AES-128-CBC + HMAC-SHA256)
Clave	Derivada del Machine ID vía PBKDF2
Alcance	Copiar profiles.json a otra máquina no descifra nada
Secretos de alertas	Contraseña SMTP y token de Telegram también cifrados

▲ **Modelo de amenaza honesto: es cifrado ligado al equipo.** Quien pueda ejecutar la app en esa misma máquina puede descifrar (la app debe hacerlo para conectarse). Protege contra el robo del archivo, no contra un administrador local.

CAPÍTULO

04 - Licenciamiento criptográfico

Firma asimétrica: el binario solo puede verificar licencias, nunca generarlas.

Las licencias se firman con **Ed25519** (criptografía de clave pública). El ejecutable lleva embebida **solo la clave pública**; la clave privada vive exclusivamente en el generador del vendedor y nunca se distribuye.

› Extraer o descompilar el binario **no** permite fabricar licencias.

› Verificación 100% **offline** : sin servidor de activación.

› Licencia ligada a un **Machine ID** estable, derivado de identificadores de hardware.

- › **Suscripción anual** : el vencimiento y el límite de bases van firmados en la propia clave.
- › Periodo de gracia y vencimiento robustos ante manipulación del reloj (marca de agua de fecha firmada).

CAPÍTULO

05 - Autenticación y sesión

Acceso protegido cuando el dashboard es accesible por red.

CONTROL	DETALLE
Hash de contraseña	PBKDF2-HMAC-SHA256 , 200.000 iteraciones, sal aleatoria
Anti fuerza bruta	5 intentos fallidos → bloqueo temporal por IP
Cookie de sesión	HttpOnly + SameSite=Lax (+ Secure con TLS)
Firma de sesión	Clave derivada de un secreto interno + Machine ID

CAPÍTULO

06 - Seguridad de red

Por defecto, expuesto al mínimo. El acceso en red es una decisión explícita.

- › Escucha solo en **127.0.0.1** por defecto, en todos los modos.
- › Exponer en red requiere un opt-in explícito (**OHD_BIND_HOST=0.0.0.0**).
- › Para acceso multiusuario: proxy inverso con **HTTPS** (IIS/ARR, nginx, Caddy).
- › El endpoint de salud (**/api/health**) no expone datos sensibles.

✕ Recomendación de auditoría: nunca publicar en HTTP plano en una red abierta. Usar TLS terminado en proxy o acceso local por RDP.

CAPÍTULO

07 - Datos y privacidad

Tus datos no salen de tu infraestructura.

- › **Sin telemetría** : el producto no envía datos de uso a ningún servidor.
- › Todo el estado (config, historial, logs) se guarda **localmente** .
- › El historial almacena métricas agregadas, no contenido de tus tablas.
- › Las alertas (email/Telegram) solo se envían a los destinatarios que tú configuras.

CAPÍTULO

08 - Cadena de suministro

Builds reproducibles y dependencias controladas.

- › Dependencias **fijadas** a versiones conocidas (requirements.txt).
- › Prevención de **XSS** : todo dato proveniente de Oracle se escapa antes de renderizar.
- › Imagen Docker basada en **python:3.12-slim** , ejecutando como usuario no-root.
- › La clave privada de licencias está excluida de todo artefacto (.gitignore / .dockerignore).