Cerrando la Brecha de Disponibilidad Disponibilidad

Un switchover “exitoso” no es una aplicación funcionando.
MAA nivel Gold — RAC, Active Data Guard, Fast-Start Failover — validado de la única forma que cuenta: que cuenta: con simulacros, medido en el cliente.

MIRACLE

Francisco Munoz Alvarez

- Over Three decades keeping mission-critical Oracle platforms alive — Maximum Availability Architecture
- Advisor to enterprises worldwide on high availability and disaster recovery
- International keynote speaker, MBA — author of the forthcoming book Engineering Resilience: The High Availability Mindset
- Races for Australia at the Dragon Boat World Championships

francisco.munoz.alvarez@miracleltd.com

https://www.linkedin.com/in/franciscomunozalvarez

fcomunoz

Contenido

01 El laboratorio — anatomía de Gold

02 El cliente decide la interrupción

03 Los simulacros — lo que “Ready: Yes” escondió

04 Veredictos, IA y el checklist

05 Las herramientas — CrashSimulator y DRRA

01

El laboratorio — anatomía de Gold

Anatomía de Gold — el laboratorio de esta charla

RAC para HA local · Active Data Guard para DR · Fast-Start Failover para transiciones de rol automatizadas

SITIO A — PRIMARIO · RAC

rac26n1 · rac26n2

Dos instancias 26ai, una base de datos. Servicios basados en rol: `crashsim_ac` · `crashsim_tac` · `racpdb_rw`.

ACTIVE DATA GUARD

redo · aplicación en tiempo real

El redo fluye al standby y se aplica al llegar — la copia de DR está al día en segundos, no al último log switch.

SITIO B — STANDBY

rac26sb

Standby físico, abierto en solo lectura — consultable, parchable, y a una transición de rol de ser primario.

FAST-START FAILOVER

Los observers `obs_n1` · `obs_n2` · `obs_sb` vigilan ambos sitios y arbitran las transiciones de rol.

CLIENTES

Se conectan a un **nombre de servicio** mediante una lista de direcciones de dos sitios — nunca a un host.

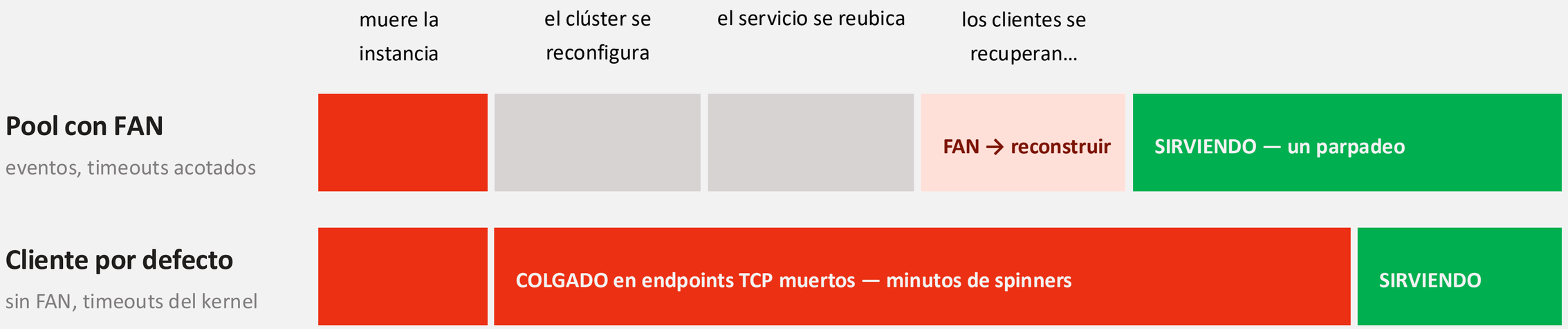
Cada caja es una capacidad candidata — hasta que un simulacro la mide.

02

El cliente decide la interrupción

Misma falla, dos interrupciones distintas

La muerte de una instancia, vista por un pool consciente de FAN vs un cliente por defecto — esquema de línea de tiempo, no a escala



La base de datos se comportó **idénticamente** en ambos carriles. La interrupción que sintieron sus usuarios la decidió la configuración del cliente — **años antes, quien escribió el connect string.**

Anatomía de un connect string resiliente

El descriptor real del laboratorio — el que usa la sonda de medición, porque es lo que usaría un cliente correcto

```
(DESCRIPTION=
  (CONNECT_TIMEOUT=5)(TRANSPORT_CONNECT_TIMEOUT=3)(RETRY_COUNT=3)  (FAILOVER=ON)
  (ADDRESS_LIST=(LOAD_BALANCE=OFF)
    (ADDRESS=(PROTOCOL=TCP)(HOST=rac26-scan)(PORT=1521))   ← Sitio A: SCAN del RAC
    (ADDRESS=(PROTOCOL=TCP)(HOST=rac26sb)(PORT=1521))      ← Sitio B: standby
  )
  (CONNECT_DATA=(SERVICE_NAME=crashsim_ac))                ← un servicio BASADO EN ROL
```

Todos los timeouts acotados

Un sitio muerto cuesta segundos — no la paciencia de TCP.

Ambos sitios, un descriptor

El cliente nunca sabe quién es primario — encuentra el servicio donde corra.

Solo nombre de servicio

Corre solo donde el rol es PRIMARY. Sin hosts. Sin SIDs. Sin ediciones a las 3 a.m.

La escalera de configuración del cliente

Cada peldaño es un cambio de servicio/conexión, no una reescritura — y cada uno reduce lo que el usuario siente

4 · Transparent Application Continuity (TAC) la base decide los límites de replay — cero cambios en la app	**el usuario siente: nada** — trabajo en vuelo repetido
3 · Application Continuity (AC) el driver graba y repite; el resultado del commit se responde	**el usuario siente: un spinner más largo**
2 · FAN + Fast Connection Failover los pools reaccionan a eventos, drenan y se reconstruyen	**el usuario siente: segundos** — nuevo OK, en vuelo falla
1 · Lista de direcciones de dos sitios, acotada failover solo al conectar — ayuda a conexiones NUEVAS	**el usuario siente: errores** en todo lo que está en vuelo
0 · Un hostname, timeouts por defecto la mayoría de los entornos hoy	**el usuario siente: minutos — Redescubrir el desastre**

03

Los simulacros — lo que “Ready: Yes” escondió

Misma falla, tres destinos — la matriz de perfiles de cliente

Tres sesiones persistentes trabajando cuando muere la instancia 1. La única variable es la configuración de conexión.

PLAIN un host, sin configuración de failover	**MURIÓ** — error a la aplicación · trabajo en vuelo **perdido**
Estilo TAF failover de sesión	**SOBREVIVIÓ** — sesión movida a la instancia 2 · trabajo en vuelo **con rollback**
TAC `crashsim_tac` servicio con Transparent Application Continuity	**SOBREVIVIÓ** — sesión movida · trabajo en vuelo **REPETIDO** · la aplicación nunca vio un error

```
# canario de servicio, cada 2s vía listener: … OK OK FAIL FAIL FAIL FAIL OK OK …
→ service_rto_class=MEASURED
```

La evidencia, reproducida

Cinco formas en que “Ready for Switchover: Yes” mintió

El broker valida transporte y aplicación de redo. Todo lo de abajo vive fuera de esa responsabilidad — y cada uno rompería o degradaría una transición degradaría una transición de rol real.

1 · STANDBY REDO LOGS FANTASMA

Miembros SRL apuntando a las rutas del **primario** — cantidad y tamaño correctos, los archivos no existen. Sin aplicación en tiempo real; dato de lag con 16 h.

2 · ARCHIVOS DE CONTRASEÑAS DIVERGENTES

Un simulacro recreó un lado. Nada se queja — hasta que el switchover muere en vuelo con `ORA-01017`.

3 · SCAN LISTENERS VARADOS

Dos de tres SCAN VIPs en un nodo **sin instancia** . Tráfico de broker y observers degradado en silencio — mientras `tnsping` decía OK.

4 · OBSERVERS SIN MASTER

Tres observers FSFO registrados — todos “Backup”, ninguno Master. Estado de configuración: ERROR.

5 · SERVICIO AUSENTE EN EL STANDBY

Definido según el manual — en un solo lado. Las definiciones de servicio **no se replican con el redo** . Interrupción garantizada tras el switchover.

CADA UNO

Invisible para una revisión de configuración del lado que uno inspeccionaría. **Ruidoso en un simulacro.**

Los dos asesinos silenciosos del failover de servicios

Ambos encontrados en este laboratorio, en ambas direcciones de las transiciones de la misma semana

ASESINO 1 · NO DEFINIDO

Las definiciones de servicio no se replican

```
PRIMARY: crashsim_ac ✓ crashsim_tac ✓ racpdb_rw ✓
STANDBY: crashsim_ac ✗ crashsim_tac ✗ racpdb_rw ✓
```

Viven en el registro propio de cada clúster; el redo nunca las transporta. **Interrupción garantizada en el switchover.**

ASESINO 2 · DEFINIDO, NUNCA INICIADO

El auto-inicio por rol es “usualmente”, no “siempre”

```
Service role: PRIMARY ✓ · policy: AUTOMATIC ✓ ·
DB: OPEN READ WRITE ✓ Service crashsim_ac is not
running.
```

Tras una transición que reinicia la base, CRS puede no re-colocar los servicios. Respuesta MAA: un trigger `AFTER STARTUP ON DATABASE` que compare `database_role` — o un paso explícito del runbook.

Una revisión de configuración aprueba ambos. **Definido no es corriendo — solo un simulacro dice la verdad.**

Los recibos: un switchover “exitoso”, medido

DGMGRL: “Switchover succeeded.” El broker: “Ready: Yes.” La sonda que finge ser su aplicación:

```
# manifiesto del escenario 85 — switchover planificado, instrumentado:
scenario_85_inject_epoch=1786662200
scenario_85_recover_epoch=1786662539
service_rto_class=STILL_DOWN
service_rto_basis=el canario vio fallar el servicio y no había vuelto
cuando el simulacro dejó de observar (incl. 90s de gracia);
el RTO del servicio es de al menos 371s y aún no se conoce.
# tras la corrección (servicio creado + arranque cableado) y re-simulacro:
CANARY_OK rac26sb PRIMARY via crashsim_ac
```

Ningún número inventado. Nada de redondear un desconocido a una métrica. **“Al menos 371 segundos y aún no conocido”** es la forma honesta de una interrupción que no terminó — y la línea que convirtió una mina oculta en una corrección.

04

Veredictos, IA y el checklist

Cinco niveles — y dos preguntas distintas

El nivel es lo que su topología puede hacer. Su RTO/RPO es lo que su negocio exige. Nunca fundir las dos frases.

- **Diamond** — sistemas de ingeniería + stack completo, protección ante pérdida extrema
- **Platinum** — sistemas de ingeniería + opciones de pérdida cero
- **Gold** — RAC + Active Data Guard + Fast-Start Failover ← esta charla
- **Silver** — clustering para HA local
- **Bronze** — instancia única, backup y restore disciplinados
- **Distributed** — una clase de despliegue a través de los niveles (multi-AZ / región / país), no un sexto nivel

EJE 1 · TOPOLOGÍA

"Somos **Gold** " — una afirmación sobre la arquitectura y su comportamiento diseñado.

EJE 2 · NEGOCIO

"Cumplimos nuestro **RTO / RPO** " — un número que fijó su negocio, que solo la medición puede confirmar.

Las revisiones de disponibilidad fallan cuando estas dos frases se funden en una.

Candidato por arquitectura — evidenciado por simulacro

La revisión de configuración valida candidatos. Solo una transición de rol ejecutada y medida valida Gold.

GOLD-CANDIDATO

- RAC instalado y sano
- ADG enviando, aplicación al día
- Observers FSFO configurados
- Servicios definidos (…en el lado que usted revisó)
- `validate database: Ready — Yes`

= el diagrama y los checklists. Necesario. No suficiente.

GOLD-EVIDENCIADO — VÍA SIMULACRO EJECUTADO

- Transición de rol ejecutada — **en ambas direcciones**
- RTO del servicio **medido** en el cliente
- Servicios probados CORRIENDO tras la transición
- Comportamiento AC/TAC demostrado, no asumido
- Evidencia firmada — lista para auditoría (CPS 230 / DORA / ISO 22301)

= lo que “somos Gold” debería significar.

Un sitio de DR que no puede servir a la aplicación no es Gold — diga lo que diga el diagrama.

La IA explica. Nunca califica.

La separación que hace segura a la IA frente a un auditor

CAPA DE IA · EXPLICAR

Un hallazgo, en lenguaje claro, para un ejecutivo — con evidencia citada.

CAPA DE IA · BUSCAR

Vectorial/semántico: “ese switchover donde el servicio no arrancó” → el simulacro correcto.

CAPA DE IA · VIGILAR

ML en la base sobre señales de estabilidad de la flota — deriva que un humano no vería.

MOTORES · RTO / RPO MEDIDOS

De sondas y simulacros — deterministas, con compuerta de evidencia.

MOTORES · VEREDICTOS Y NIVELES

Misma entrada → mismo veredicto, trazable. El único lugar donde se emiten veredictos.

MOTORES · EVIDENCIA DE CUMPLIMIENTO

Firmada, con hash, lista para auditoría.

La capa de IA es de solo lectura, anclada en evidencia, cada respuesta registrada — **lee, nunca escribe, nunca juzga** . Explicar es un problema de lenguaje, perfecto para la IA. **Juzgar si la recuperación de su banco funciona, no lo es.**

El checklist y las trampas

HACER

- Servicios basados en rol en **todos** los sitios + un mecanismo de arranque (trigger o runbook)
- Descriptores de dos sitios · timeouts acotados · solo nombres de servicio
- Pools con FAN · AC/TAC en las cargas que lo ameriten
- Auditar las cinco mentiras: SRLs · archivos de contraseñas · SCAN · observers · paridad de servicios
- **Simular transiciones de rol con cadencia — en ambas direcciones — medir en el cliente, conservar la evidencia**

NO HACER

- Confiar en salidas de preparación que nunca fueron diseñadas para ver su aplicación
- Practicar failover sin practicar failback — la mitad de los hallazgos fueron en el regreso
- Dejar que “configurado” sustituya a “probado”
- Creer la frase que esta charla existe para matar: **“definido” = “corriendo”**

05

Las herramientas — CrashSimulator y DRRA

GA Release: Aug 17, 2026

CrashSimulator — Open Source Edition

Deje de esperar que su base se recupere. Ensáyelo — desde un único script Bash, con dry-run por defecto.

UN SCRIPT, SIN AGENTE

Un script Bash autocontenido y un cliente Oracle — nada que instalar, nada que comprar. Apúntelo a una base de laboratorio.

CATÁLOGO DE 123 ENTRADAS

103 escenarios de falla de base y plataforma + 20 simulacros de Autonomous DB — inyectados de verdad, reversibles, en laboratorio.

RECUPERACIÓN, NO SOLO FALLA

Cada escenario trae su runbook de recuperación y lo valida — y convierte la corrida en evidencia lista para auditoría.

Diseñado para ser difícil de usar mal: **dry-run es el modo por defecto**, toda falla es reversible. Apache-2.0 — `github.com/fmunozalvarez/crashsimulator`

```
Starting CrashSimulator Guided Workflow menu...
Trying target topology discovery for the menu header. This normally takes a few seconds on database hosts.
If SQL*Plus is unavailable, the menu still opens for ADB reports, ADB scenarios, review, and configuration.

CrashSimulator V2 2.0.3-beta-labs.89
Database: rac19db  Role: PRIMARY  Open: READ WRITE  CDB: YES
Instance: rac19db1  Storage: ASM  Cluster: RAC

Selected scenario: none
PDB: not set  Schema: not set  FILE#: not set
Manifest: not set
Log dir: /home/oracle/crashsimulator_logs
Report deep validation: 0
Baseline backup tag prefix: CSIM_BASE
Config file: /home/oracle/.crashsimulator/crashsimulator.conf
Audit retain: 1  Retention days: 365  Audit dir: /home/oracle/crashsimulator_logs/audit
Scenario 25 guards: local-only=0  max-targets=not set  piece-handle=not-set
RMAN catalog: configured
Password-file recovery: SYS password=not-set  service=not set
Scenario 61/63 knobs: FRA target=98%  FRA headroom=64MB  TEMP workload=512MB
ADB scenario: not set

Guided Workflow

Safe discovery and planning
  1. Discover or refresh database topology
  2. Select scenario
  3. List all scenarios
 11. Run health check / validation
 12. Configure targets and options
 13. Browse recent manifests, logs, reports, and inspect contents
 14. Dry-run random/aleatory scenario for this topology
 16. Reports
 17. Generate scenario readiness report for this topology
 18. Audit / retention settings
 19. Review collected topology, logs, reports, and history
 20. Autonomous Database scenarios
 21. Seed / prepare scenario lab for this topology
 22. Public readiness and safety checks
  (5 option(s) hidden - select a scenario first (option 2))

Execution actions - typed confirmation required
 15. Execute random/aleatory scenario for this topology
  (3 option(s) hidden - select a scenario first (option 2))
  q. Quit

Choice:
```

CrashSimulator Enterprise

Pruebe que su flota Oracle realmente puede recuperarse — cada afirmación calificada contra evidencia recolectada, nunca contra configuración.

MOTOR DE SIMULACROS · TODA LA FLOTA

El catálogo de 123 escenarios de falla/recuperación en todo el entorno. Recolección dual: agente en el host o recolector SQL puro sin instalación — pull, no push. Auto-actualización firmada y fail-closed.

ENTERPRISE RESILIENCE CONSOLE

Índice de Resiliencia 0–100 sobre la escalera MAA de seis peldaños — peldaños — siempre separado **candidato vs evidenciado** . Programas Programas gobernados: solicitar → aprobar → correr → validar.

EVIDENCIA Y CUMPLIMIENTO

Paquetes de evidencia con hash en un clic · 8 marcos calificados en vivo · acciones cuantificadas en dólares.

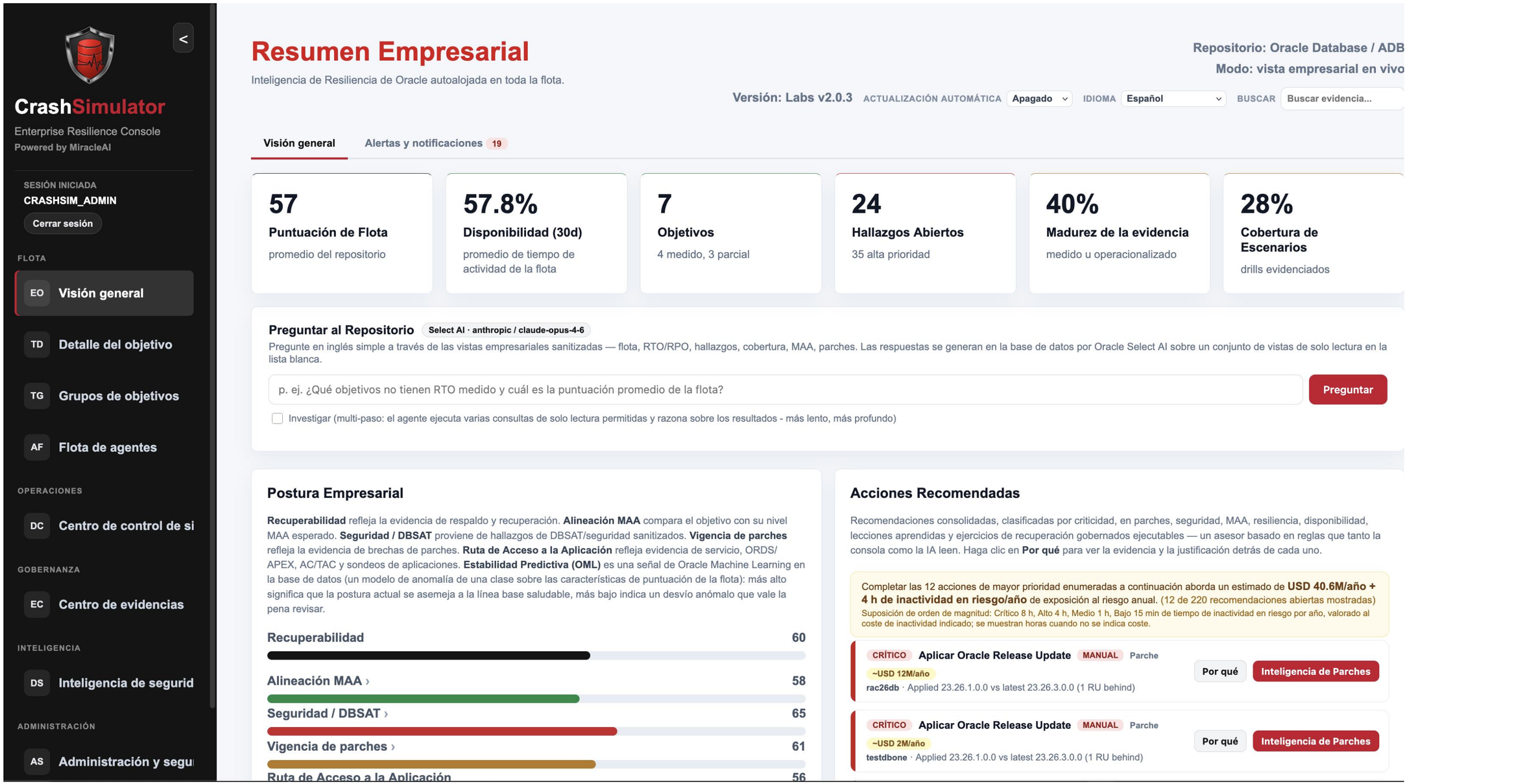
SEGURIDAD Y PARIDAD

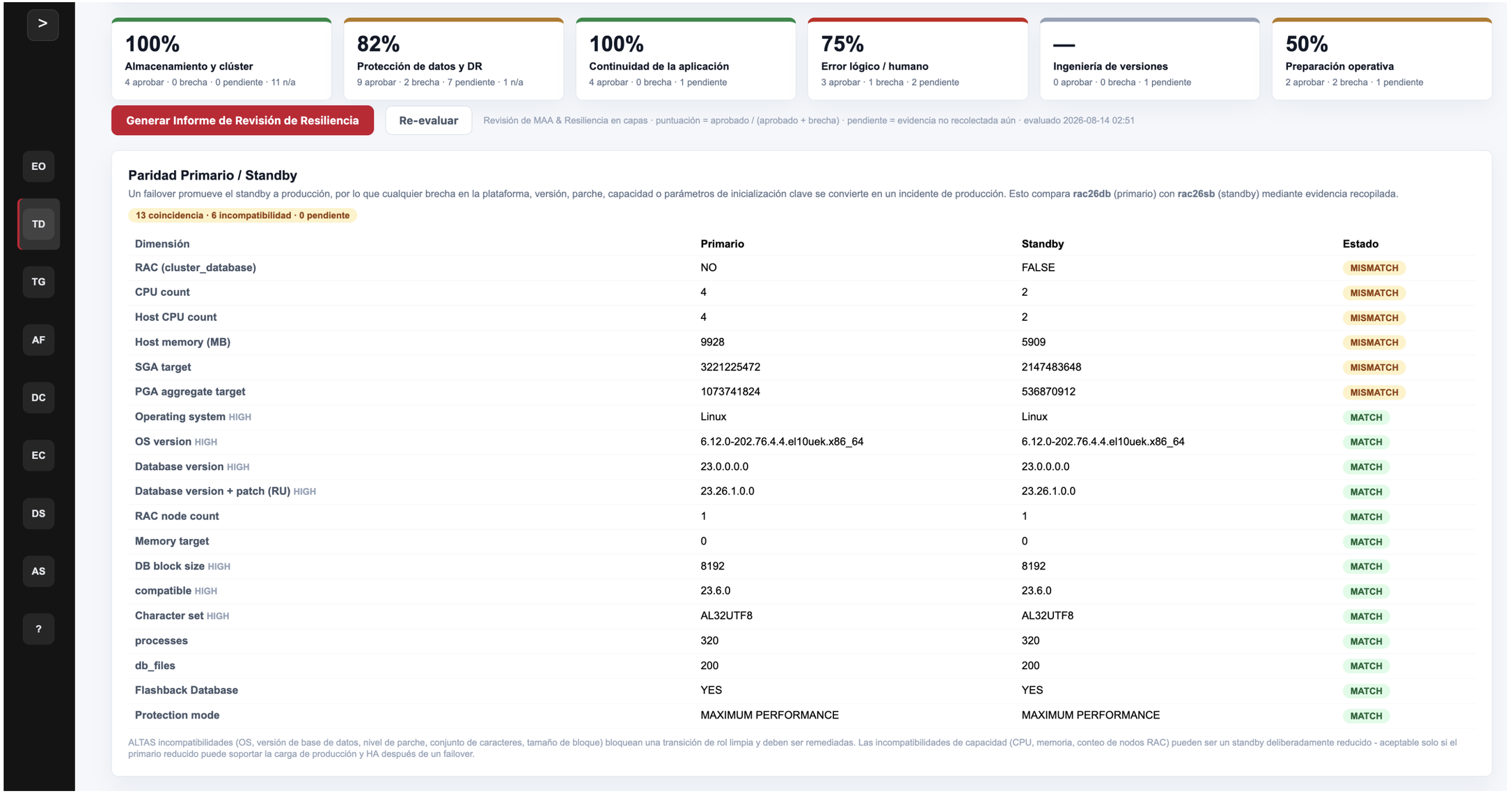
Postura derivada de DBSAT · paridad primario/standby · inteligencia de parches ponderada por CVE.

MÁS ALLÁ DE ORACLE (PRONTO)

PostgreSQL · MySQL · MongoDB · SQL Server — una calificación normalizada, con compuerta de evidencia.

La consola nunca reporta un nivel que no midió — candidato por arquitectura, evidenciado por simulacro, en toda la flota.


CrashSimulator
Enterprise Resilience Console
Powered by MiracleAI
SESIÓN INICIADA
CRASHSIM_ADMIN
Cerrar sesión
FLOTA
EO Visión general
TD Detalle del objetivo
TG Grupos de objetivos
AF Flota de agentes
OPERACIONES
DC Centro de control de si
GOBERNANZA
EC Centro de evidencias
INTELIGENCIA
DS Inteligencia de segurid
ADMINISTRACIÓN
AS Administración y segu
Resumen Empresarial
Inteligencia de Resiliencia de Oracle autoalojada en toda la flota.
Repositorio: Oracle Database / ADB
Modo: vista empresarial en vivo
Versión: Labs v2.0.3
ACTUALIZACIÓN AUTOMÁTICA
Apagado
IDIOMA
Español
BUSCAR
Buscar evidencia...
Visión general
Alertas y notificaciones 19
57
Puntuación de Flota
promedio del repositorio
57.8%
Disponibilidad (30d)
promedio de tiempo de actividad de la flota
7
Objetivos
4 medido, 3 parcial
24
Hallazgos Abiertos
35 alta prioridad
40%
Madurez de la evidencia
medido u operacionalizado
28%
Cobertura de Escenarios
drills evidenciados
Preguntar al Repositorio
Select AI · anthropic / claude-opus-4-6
Pregunte en inglés simple a través de las vistas empresariales sanitizadas — flota, RTO/RPO, hallazgos, cobertura, MAA, parches. Las respuestas se generan en la base de datos por Oracle Select AI sobre un conjunto de vistas de solo lectura en la lista blanca.
p. ej. ¿Qué objetivos no tienen RTO medido y cuál es la puntuación promedio de la flota?
Preguntar
Investigar (multi-paso: el agente ejecuta varias consultas de solo lectura permitidas y razona sobre los resultados - más lento, más profundo)
Postura Empresarial
Recuperabilidad refleja la evidencia de respaldo y recuperación. Alineación MAA compara el objetivo con su nivel MAA esperado. Seguridad / DBSAT proviene de hallazgos de DBSAT/seguridad sanitizados. Vigencia de parches refleja la evidencia de brechas de parches. Ruta de Acceso a la Aplicación refleja evidencia de servicio, ORDS/APEX, AC/TAC y sondeos de aplicaciones. Estabilidad Predictiva (OML) es una señal de Oracle Machine Learning en la base de datos (un modelo de anomalía de una clase sobre las características de puntuación de la flota): más alto significa que la postura actual se asemeja a la línea base saludable, más bajo indica un desvío anómalo que vale la pena revisar.
Recuperabilidad 60
Alineación MAA › 58
Seguridad / DBSAT › 65
Vigencia de parches › 61
Ruta de Acceso a la Aplicación 56
Acciones Recomendadas
Recomendaciones consolidadas, clasificadas por criticidad, en parches, seguridad, MAA, resiliencia, disponibilidad, lecciones aprendidas y ejercicios de recuperación gobernados ejecutables — un asesor basado en reglas que tanto la consola como la IA leen. Haga clic en Por qué para ver la evidencia y la justificación detrás de cada uno.
Completar las 12 acciones de mayor prioridad enumeradas a continuación aborda un estimado de USD 40.6M/año + 4 h de inactividad en riesgo/año de exposición al riesgo anual. (12 de 220 recomendaciones abiertas mostradas)
Suposición de orden de magnitud: Crítico 8 h, Alto 4 h, Medio 1 h, Bajo 15 min de tiempo de inactividad en riesgo por año, valorado al coste de inactividad indicado; se muestran horas cuando no se indica coste.
CRÍTICO Aplicar Oracle Release Update MANUAL Parche
~USD 12M/año
rac26db · Applied 23.26.1.0.0 vs latest 23.26.3.0.0 (1 RU behind)
Por qué
Inteligencia de Parches
CRÍTICO Aplicar Oracle Release Update MANUAL Parche
~USD 2M/año
testdbone · Applied 23.26.1.0.0 vs latest 23.26.3.0.0 (1 RU behind)
Por qué
Inteligencia de Parches


>
EO
TD
TG
AF
DC
EC
DS
AS
?
100%
Almacenamiento y clúster
4 aprobar · 0 brecha · 0 pendiente · 11 n/a
82%
Protección de datos y DR
9 aprobar · 2 brecha · 7 pendiente · 1 n/a
100%
Continuidad de la aplicación
4 aprobar · 0 brecha · 1 pendiente
75%
Error lógico / humano
3 aprobar · 1 brecha · 2 pendiente
—
Ingeniería de versiones
0 aprobar · 0 brecha · 1 pendiente
50%
Preparación operativa
2 aprobar · 2 brecha · 1 pendiente
Generar Informe de Revisión de Resiliencia
Re-evaluar
Revisión de MAA & Resiliencia en capas · puntuación = aprobado / (aprobado + brecha) · pendiente = evidencia no recolectada aún · evaluado 2026-08-14 02:51
Paridad Primario / Standby
Un failover promueve el standby a producción, por lo que cualquier brecha en la plataforma, versión, parche, capacidad o parámetros de inicialización clave se convierte en un incidente de producción. Esto compara rac26db (primario) con rac26sb (standby) mediante evidencia recopilada.
13 coincidencia · 6 incompatibilidad · 0 pendiente
Dimensión
Primario
Standby
Estado
RAC (cluster_database)
NO
FALSE
MISMATCH
CPU count
4
2
MISMATCH
Host CPU count
4
2
MISMATCH
Host memory (MB)
9928
5909
MISMATCH
SGA target
3221225472
2147483648
MISMATCH
PGA aggregate target
1073741824
536870912
MISMATCH
Operating system HIGH
Linux
Linux
MATCH
OS version HIGH
6.12.0-202.76.4.4.el10uek.x86_64
6.12.0-202.76.4.4.el10uek.x86_64
MATCH
Database version HIGH
23.0.0.0.0
23.0.0.0.0
MATCH
Database version + patch (RU) HIGH
23.26.1.0.0
23.26.1.0.0
MATCH
RAC node count
1
1
MATCH
Memory target
0
0
MATCH
DB block size HIGH
8192
8192
MATCH
compatible HIGH
23.6.0
23.6.0
MATCH
Character set HIGH
AL32UTF8
AL32UTF8
MATCH
processes
320
320
MATCH
db_files
200
200
MATCH
Flashback Database
YES
YES
MATCH
Protection mode
MAXIMUM PERFORMANCE
MAXIMUM PERFORMANCE
MATCH
ALTAS incompatibilidades (OS, versión de base de datos, nivel de parche, conjunto de caracteres, tamaño de bloque) bloquean una transición de rol limpia y deben ser remediadas. Las incompatibilidades de capacidad (CPU, memoria, conteo de nodos RAC) pueden ser un standby deliberadamente reducido - aceptable solo si el primario reducido puede soportar la carga de producción y HA después de un failover.

Continuidad y radio de explosión

Continuidad del throughput y contención del radio de explosión del último drill de continuidad de servicio AC/TAC/FAN. Solo se demuestra a partir de un drill con carga de trabajo en curso.

Contenido | Carga de trabajo presente | Canario sintético

60.2% caída de throughput — MTTD — tiempo hasta la línea base

Demostrado con una carga de trabajo de canario sintético. Vuelva a ejecutar con tráfico de aplicación real para obtener evidencia de nivel de producción.

Medido 2026-08-13 17:23 UTC — el último drill que capturó evidencia de continuidad. Un drill posterior que no registró ninguna no modifica estas cifras.

Explicar este gráfico con IA

Simulacros ejecutados (últimos 90 días)

Incluye drills orquestados a través del pipeline gobernado del repositorio y drills ejecutados directamente en el destino con la CLI de CrashSimulator (atestiguados por el operador, detectados y enviados por el agente). La columna **Ejecutado por** indica cuál.

ESCENARIO	ETAPA	RESULTADO	EJECUTADO POR	INICIADO	TERMINADO	RTO DE SERVICIO	RTO DE RESTAURACIÓN	RPO	CADENA DE ARCHIVADO	COBERTURA DE COPIAS
91	EXECUTED	EXECUTED	Repositorio — gobernado	2026-08-14 05:53 +00:00	2026-08-14 05:53 +00:00	Sin interrupción	not set	Sin datos en riesgo	—	—
64	EXECUTED	RECOVERY_PENDING	Repositorio — gobernado	2026-08-14 02:51 +00:00	2026-08-14 02:51 +00:00	—	not set	not set	—	—
65	EXECUTED	RECOVERY_PENDING	Repositorio — gobernado	2026-08-14 02:43 +00:00	2026-08-14 02:43 +00:00	—	not set	not set	—	—
91	EXECUTED	PASS	Destino — directo	2026-08-12 04:59 +00:00	2026-08-12 05:13 +00:00	Sin interrupción	14m 21s	Sin datos en riesgo	—	—
91	EXECUTED	PASS	Destino — directo	2026-08-12 03:57 +00:00	2026-08-12 04:11 +00:00	Sin interrupción	14m 16s	Sin datos en riesgo	—	—
56	EXECUTED	PASS	Destino — directo	2026-08-12 02:51 +00:00	2026-08-12 02:52 +00:00	Sin interrupción	50s	Sin datos en riesgo	—	—
55	EXECUTED	PASS	Destino — directo	2026-08-12 01:13 +00:00	2026-08-12 01:22 +00:00	12s	8m 37s	zero	—	—
55	EXECUTED	PASS	Destino — directo	2026-08-11 13:02 +00:00	2026-08-11 13:21 +00:00	Sin interrupción	19m 5s	zero	—	—
91	EXECUTED	PASS	Destino — directo	2026-08-11 11:12 +00:00	2026-08-11 11:22 +00:00	Sin interrupción	9m 49s	Sin datos en riesgo	—	—
91	CLOSED	PASS	Repositorio — gobernado	2026-08-11 04:06 +00:00	2026-08-11 10:34 +00:00	Sin interrupción	not set	Sin datos en riesgo	—	—
56	EXECUTED	PASS	Destino — directo	2026-08-11 09:27 +00:00	2026-08-11 09:29 +00:00	20s	1m 49s	Sin datos en riesgo	—	—

MIRACLE

DRRA — Data Resilience Review Assistant

Convierta una conversación en prueba de resiliencia — sin consultor, sin un mes, sin conexión a sus bases de datos.

1 · ENTREVISTA

Un chat adaptativo — 110+ preguntas, solo las relevantes para su arquitectura. Pausar, retomar y revisar cuando quiera.

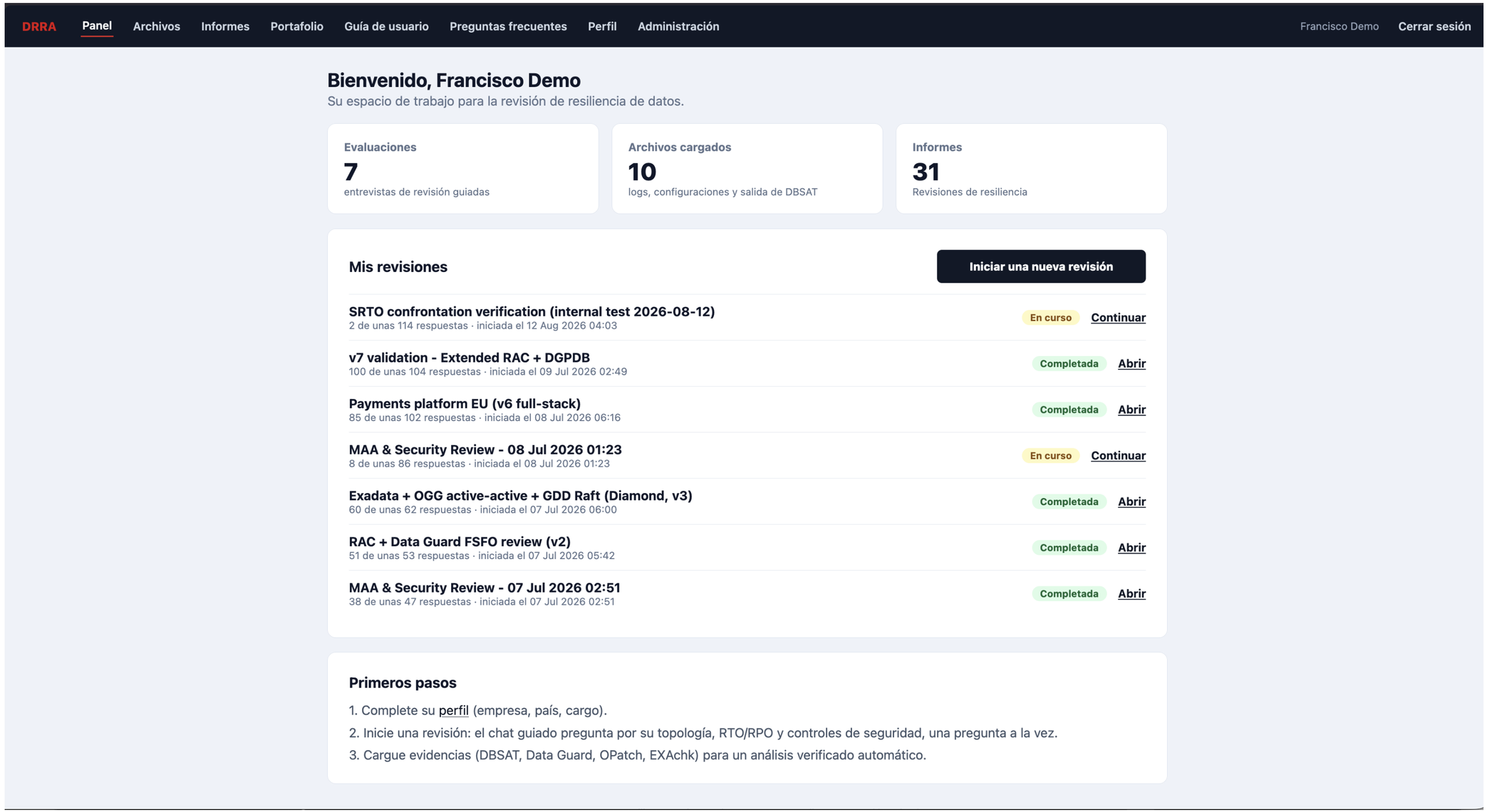
2 · EVIDENCIA (OPCIONAL)

Suba logs, salida de DBSAT, inventarios de OPatch. Las afirmaciones que su evidencia contradice se **degradan, no se maquillan**.

3 · INFORME

Autocontenido, con hash SHA-256. Nivel MAA en **tres ejes** : requerido por SLA · candidato · evidenciado — más una hoja de ruta Ahora/Próximo/Después.

Gratuito · nada que instalar · 8 marcos calificados con honestidad · 13 idiomas


DRRA
Panel
Archivos
Informes
Portafolio
Guía de usuario
Preguntas frecuentes
Perfil
Administración
Francisco Demo
Cerrar sesión
Bienvenido, Francisco Demo
Su espacio de trabajo para la revisión de resiliencia de datos.
Evaluaciones
7
entrevistas de revisión guiadas
Archivos cargados
10
logs, configuraciones y salida de DBSAT
Informes
31
Revisiones de resiliencia
Mis revisiones
Iniciar una nueva revisión
SRTO confrontation verification (internal test 2026-08-12)
2 de unas 114 respuestas · iniciada el 12 Aug 2026 04:03
En curso
Continuar
v7 validation - Extended RAC + DGPDB
100 de unas 104 respuestas · iniciada el 09 Jul 2026 02:49
Completada
Abrir
Payments platform EU (v6 full-stack)
85 de unas 102 respuestas · iniciada el 08 Jul 2026 06:16
Completada
Abrir
MAA & Security Review - 08 Jul 2026 01:23
8 de unas 86 respuestas · iniciada el 08 Jul 2026 01:23
En curso
Continuar
Exadata + OGG active-active + GDD Raft (Diamond, v3)
60 de unas 62 respuestas · iniciada el 07 Jul 2026 06:00
Completada
Abrir
RAC + Data Guard FSFO review (v2)
51 de unas 53 respuestas · iniciada el 07 Jul 2026 05:42
Completada
Abrir
MAA & Security Review - 07 Jul 2026 02:51
38 de unas 47 respuestas · iniciada el 07 Jul 2026 02:51
Completada
Abrir
Primeros pasos
1. Complete su perfil (empresa, país, cargo).
2. Inicie una revisión: el chat guiado pregunta por su topología, RTO/RPO y controles de seguridad, una pregunta a la vez.
3. Cargue evidencias (DBSAT, Data Guard, OPatch, EXAchk) para un análisis verificado automático.

componente?

Around 30 seconds of committed data loss is acceptable for pure component failures, per our ops agreement.

¿Cuál es el RTO máximo tolerable para DESASTRES: pérdida completa de la base de datos, sitio o región?

Minutes

¿Cuál es la máxima pérdida de datos tolerable (RPO) ante desastres?

Near zero (seconds)

¿Qué tiempo de inactividad se asigna para el mantenimiento PLANIFICADO (cambios en la base de datos, infraestructura de grid y aplicaciones)?

Hours per window

¿Cuál es el tiempo de recuperación objetivo (RTO) para un escenario de CIBER / ransomware (recuperación aislada y validada como limpia)?

Up to one day

Para la recuperación cibernética, ¿qué punto de recuperación es aceptable?

El RPO cibernético realista es el ÚLTIMO PUNTO LIMPIO VALIDADO, que depende de copias inmutables y la cadencia de validación - no de la replicación.

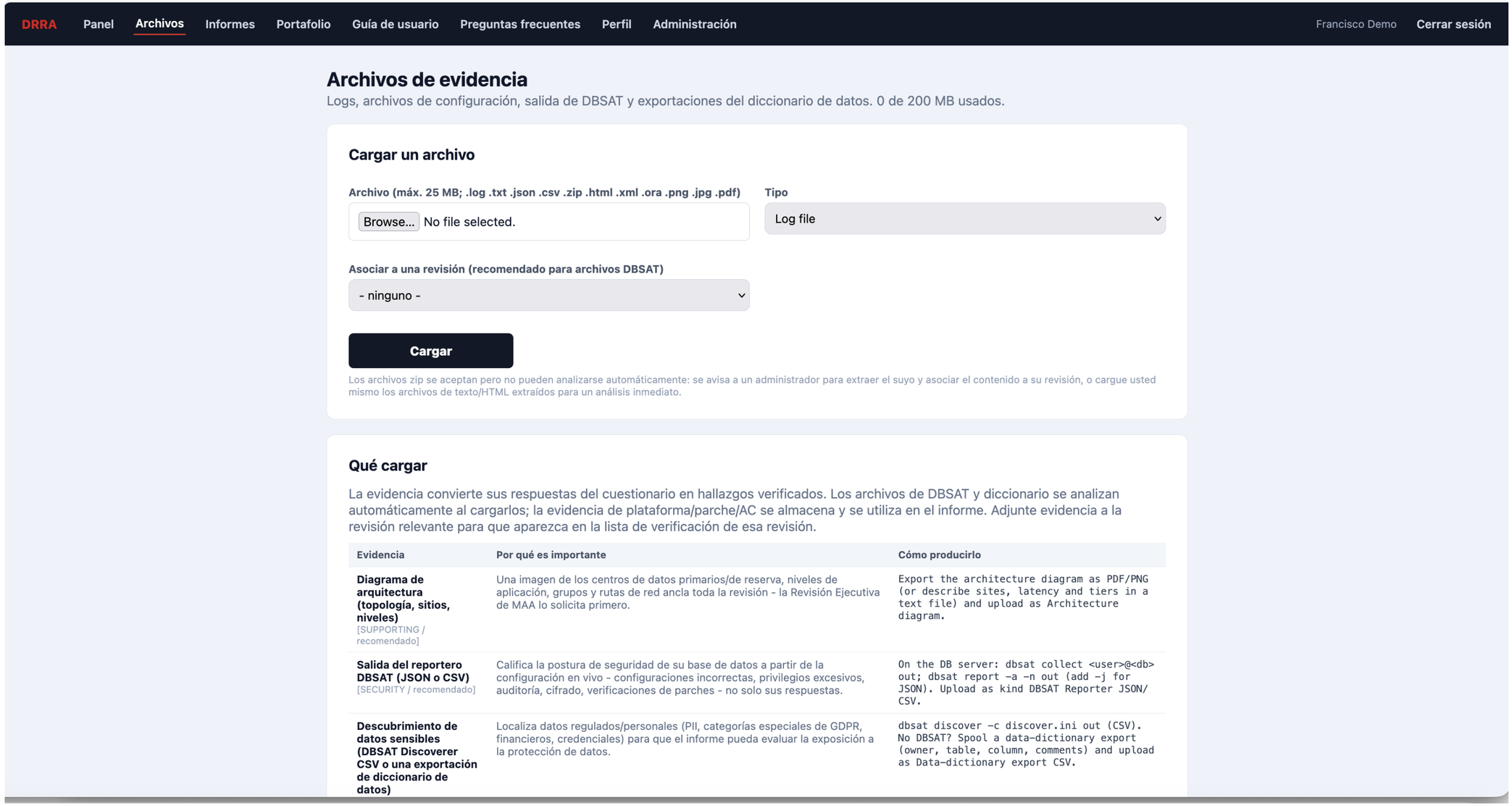
Último punto de recuperación limpio validado (copia inmutable) | **Última copia de seguridad, limpia o no** | **No definido**

Otro - escribir mi propia respuesta

Explicar esta pregunta con IA

How do I find this?

← Change my previous answer


DRRA
Panel
Archivos
Informes
Portafolio
Guía de usuario
Preguntas frecuentes
Perfil
Administración
Francisco Demo
Cerrar sesión
Archivos de evidencia
Logs, archivos de configuración, salida de DBSAT y exportaciones del diccionario de datos. 0 de 200 MB usados.
Cargar un archivo
Archivo (máx. 25 MB; .log .txt .json .csv .zip .html .xml .ora .png .jpg .pdf)
Browse... No file selected.
Tipo
Log file
Asociar a una revisión (recomendado para archivos DBSAT)
- ninguno -
Cargar
Los archivos zip se aceptan pero no pueden analizarse automáticamente: se avisa a un administrador para extraer el suyo y asociar el contenido a su revisión, o cargue usted mismo los archivos de texto/HTML extraídos para un análisis inmediato.
Qué cargar
La evidencia convierte sus respuestas del cuestionario en hallazgos verificados. Los archivos de DBSAT y diccionario se analizan automáticamente al cargarlos; la evidencia de plataforma/parche/AC se almacena y se utiliza en el informe. Adjunte evidencia a la revisión relevante para que aparezca en la lista de verificación de esa revisión.
Evidencia
Por qué es importante
Cómo producirlo
Diagrama de arquitectura (topología, sitios, niveles)
[SUPPORTING / recomendado]
Una imagen de los centros de datos primarios/de reserva, niveles de aplicación, grupos y rutas de red ancla toda la revisión - la Revisión Ejecutiva de MAA lo solicita primero.
Export the architecture diagram as PDF/PNG (or describe sites, latency and tiers in a text file) and upload as Architecture diagram.
Salida del reportero DBSAT (JSON o CSV)
[SECURITY / recomendado]
Califica la postura de seguridad de su base de datos a partir de la configuración en vivo - configuraciones incorrectas, privilegios excesivos, auditoría, cifrado, verificaciones de parches - no solo sus respuestas.
On the DB server: dbsat collect <user>@<db> out; dbsat report -a -n out (add -j for JSON). Upload as kind DBSAT Reporter JSON/CSV.
Descubrimiento de datos sensibles (DBSAT Discoverer CSV o una exportación de diccionario de datos)
Localiza datos regulados/personales (PII, categorías especiales de GDPR, financieros, credenciales) para que el informe pueda evaluar la exposición a la protección de datos.
dbsat discover -c discover.ini out (CSV). No DBSAT? Spool a data-dictionary export (owner, table, column, comments) and upload as Data-dictionary export CSV.

ORACLE RESILIENCE REVIEW ASSISTANT

Revisión de Resiliencia Completa

MAA & Security Review - 07 Jul 2026 02:51

Preparado para: **Francisco Demo**, CloudDB (Australia) · Generado: 2026-07-17 03:14 +00:00

Resumen ejecutivo

Esta Revisión de Resiliencia Completa de **Finance PROD database FINPRD, core payments application** se basa en **38** respuestas y **3** archivo(s) de evidencia cargado(s). El negocio exige disponibilidad de nivel **Gold**; la arquitectura instalada podría ofrecer **Bronze**; la evidencia probada respalda hoy **Bronze**.

42/100

Índice de Resiliencia

20 x el promedio de las puntuaciones de dominio evaluadas - un número para rastrear entre revisiones. Resume la matriz de evidencia; los niveles y hallazgos a continuación lo explican.

Esta revisión puntúa en o por encima del 0 por ciento de las 4 otras revisiones completadas en esta plataforma (comparación anónima y agregada).

3 Crítico 6 Alto 7 Medio 0 Bajo · verificación: 0 confirmadas, 2 contradichas

Requisitos clave del negocio: RTO local Minutes · RTO ante desastre Minutes · RPO Near zero (seconds) · conmutación por error Automatic failover required · degradación tolerada Up to 20%

Hallazgos principales:

- Crítico **La disponibilidad evidenciada se encuentra dos o más niveles MAA por debajo del requisito de negocio** — Los compromisos de RTO/RPO del negocio no pueden cumplirse actualmente; la exposición es continua hasta que se subsane.
- Crítico **No existe un sitio de recuperación ante desastres para un RTO del orden de minutos** — Una pérdida del sitio o de la base de datos implica una recuperación a partir de copia de seguridad: de horas a días, con pérdida de datos hasta la última copia de seguridad.
- Crítico **Los datos en reposo no están cifrados (TDE deshabilitado)** — Los medios de almacenamiento, las copias de seguridad y los clones exponen datos legibles; exposición conforme al Art. 32 del GDPR.
- Alto **Base de datos de instancia única con un RTO local del orden de minutos** — Una falla de instancia o nodo provoca una interrupción total hasta que se realice un reinicio manual o una restauración.
- Alto **DBSAT: Transparent Data Encryption** — Reportado directamente por Oracle DBSAT contra la configuración activa.

Alineación MAA: La arquitectura actual puede lograr como máximo Bronze mientras que el requisito es Gold - una brecha arquitectónica que la validación por sí sola no puede cerrar.

contradichas: Declarado: “No” - la evidencia muestra: “2”.

contradichas: Declarado: “No” - la evidencia muestra: “1”.

Comenzar con: Encargue una hoja de ruta de elevación MAA: flujos de trabajo de arquitectura, configuración y validación para cerrar la brecha de nivel. Servicio sugerido: consultoría de arquitectura MAA / proyecto de elevación de nivel.

AI-detected highlights from your answers:

- **No Standby Database SPOF** - Single point of failure: no standby database currently in place
- **Patching Backlog Exists** - Patching backlog identified as a top availability/security risk
- **No DR Site Critical Gap** - Minutes-or-better DR required but no DR site; interim plan is RMAN restore to spare host

MIRACLE

Hallazgos y riesgos

Crítico **La disponibilidad evidenciada se encuentra dos o más niveles MAA por debajo del requisito de negocio** [MAA / BUSINESS_REQ / confidence HIGH]

Observación: Los requisitos de negocio exigen GOLD, pero la evidencia comprobada solo respalda BRONZE.

Impacto: Los compromisos de RTO/RPO del negocio no pueden cumplirse actualmente; la exposición es continua hasta que se subsane.

Recomendación: Encargue una hoja de ruta de elevación MAA: flujos de trabajo de arquitectura, configuración y validación para cerrar la brecha de nivel. Servicio sugerido: consultoría de arquitectura MAA / proyecto de elevación de nivel.

Referencia de buenas prácticas: Oracle Maximum Availability Architecture (MAA) Best Practices & Reference Architectures

Crítico **No existe un sitio de recuperación ante desastres para un RTO del orden de minutos** [MAA / SITE_DR / confidence HIGH]

Observación: El negocio requiere recuperación ante desastres en minutos, pero no existe ninguna base de datos en espera. Plan provisional: restaurar a partir de copias de seguridad nocturnas de RMAN en un host disponible; proyecto de DR planificado para el cuarto trimestre.

Impacto: Una pérdida del sitio o de la base de datos implica una recuperación a partir de copia de seguridad: de horas a días, con pérdida de datos hasta la última copia de seguridad.

Recomendación: Implemente (Active) Data Guard con Broker y servicios basados en roles; valide mediante una conmutación (switchover) medida. Servicio sugerido: proyecto de implementación de Data Guard / DR.

Referencia de buenas prácticas: Oracle Data Guard Concepts and Administration

Crítico **Los datos en reposo no están cifrados (TDE deshabilitado)** [SECURITY / SEC_POSTURE / confidence HIGH]

Observación: TDE no está habilitado a pesar de haberse detectado datos de categoría especial según el GDPR (2 columnas).

Impacto: Los medios de almacenamiento, las copias de seguridad y los clones exponen datos legibles; exposición conforme al Art. 32 del GDPR.

Recomendación: Habilite el cifrado de tablespaces con TDE; combínelo con copias de seguridad cifradas. Servicio sugerido: proyecto de bastionado de seguridad.

Referencia de buenas prácticas: Oracle Database Security Guide (TDE, unified auditing, least privilege, network encryption)

Alto **Base de datos de instancia única con un RTO local del orden de minutos** [MAA / LOCAL_HA / confidence HIGH]

Observación: Las fallas locales requieren recuperación en minutos, pero la base de datos es de instancia única.

Impacto: Una falla de instancia o nodo provoca una interrupción total hasta que se realice un reinicio manual o una restauración.

Recomendación: Introduzca RAC (o, como mínimo, reinicio gestionado por clúster junto con un runbook de recuperación local ensayado). Servicio sugerido: implementación de RAC / alta disponibilidad local.

Referencia de buenas prácticas: Oracle Real Application Clusters Administration and Deployment Guide

Alto **DBSAT: Transparent Data Encryption** [SECURITY / ENCRYPTION / confidence HIGH]

Observación: Hallazgo de DBSAT CRYPT.TDE (Cifrado).

Impacto: Reportado directamente por Oracle DBSAT contra la configuración activa.

Recomendación: Cifre los tablespaces que contienen datos sensibles con TDE.

Referencia de buenas prácticas: Oracle Maximum Availability Architecture (MAA) Best Practices & Reference Architectures

Postura de seguridad (DBSAT)

Área de riesgo	Hallazgos	Alto	Medio / Evaluar
PRIVILEGES	2	1	1
AUTHENTICATION	2	1	1
ENCRYPTION	1	1	0
AUDITING	1	0	1
MISCONFIG	1	0	0

Descubrimiento de datos sensibles

Categoría	Sensibilidad	Columnas	Idioma(s) del diccionario
Credentials / secrets	CRITICAL	1	IT
Payment card number (PCI)	CRITICAL	1	ES
Health / medical data **Categoría especial RGPD Art.9**	CRITICAL	2	EN, IT
Date of birth	HIGH	2	DE, PT
Salary / compensation	HIGH	1	EN
Bank account / IBAN	HIGH	1	EN
Person name	MEDIUM	1	EN
Phone number	MEDIUM	1	NL

Alineación de cumplimiento normativo

CIS Oracle Database Benchmark — 1 pass · 1 partial · 2 fail · 2 unknown

- **FAIL** **CIS 4** Cuentas de usuario y configuraciones de perfil (DBSAT findings: 1 high, 1 medium/evaluate, 0 pass/low)
- **FAIL** **CIS 5** Privilegios, concesiones y ACLs (DBSAT findings: 1 high, 1 medium/evaluate, 0 pass/low)
- **PARTIAL** **CIS 6** Políticas de auditoría (DBSAT findings: 0 high, 1 medium/evaluate, 0 pass/low)

APRA CPS 230 Gestión de Riesgos Operacionales (Australia) — 1 pass · 0 partial · 3 fail · 4 unknown

- **FAIL** **CPS230-BCP** Plan de continuidad del negocio creíble y actualizado (libros de ejecución mantenidos) (OPS_RUNBOOKS=NONE (expected CURRENT);)
- **FAIL** **CPS230-CYBER** Recuperación de eventos cibernéticos a un punto limpio validado dentro de la tolerancia (BK_IMMUTABLE=N (expected Y);)
- **FAIL** **CPS230-TEST** Plan de continuidad probado contra escenarios severos pero plausibles (OPS_DRILLS=NEVER (expected IN:ANNUAL|QUARTERLY);)

Se decide en el cliente. Se prueba con simulacros.

La disponibilidad se decide en el cliente, se prueba con simulacros y se paga por minuto. Preguntas bienvenidas.

MIRACLE

Together we make miracles

Thank You!

Francisco Munoz Alvarez
Global CTO & Chief Evangelist

francisco.munoz.alvarez@miracleltd.com
https://www.linkedin.com/in/franciscomunozalvarez
fcomunoz

MIRACLE