

O CHECKLIST DE OBSERVABILIDADE QUE FAZ VOCÊ ACHAR O BUG EM MINUTOS.

24 itens em 6 blocos. Marque cada um no seu serviço. No fim, o checklist rápido antes de subir uma rota nova.

LOGS

- ☐ **01** Log estruturado em JSON (nível, mensagem, horário, serviço, versão). Nada de print solto.
- ☐ **02** Todo log de requisição carrega o request_id e o trace_id.
- ☐ **03** Nível certo: ERROR só para o que exige ação; DEBUG desligado em produção.
- ☐ **04** Nunca logar senha, token, cartão ou dado pessoal sem máscara.

MÉTRICAS

- ☐ **05** Os 4 sinais de ouro em todo serviço: latência, tráfego, erros e saturação.
- ☐ **06** Latência em histograma (p50, p95, p99), não só a média.
- ☐ **07** Métrica de negócio: pedidos, pagamentos ou cadastros por minuto.
- ☐ **08** Nomes e labels padronizados; nada de ID de usuário como label (explode a cardinalidade).

TRACES

- ☐ **09** OpenTelemetry instrumentando HTTP, banco de dados e fila.
- ☐ **10** Contexto propagado entre serviços (cabeçalho traceparent do W3C Trace Context).
- ☐ **11** Span em toda chamada externa, com o tempo de cada uma.
- ☐ **12** Link do trace no log de erro: do erro ao trace em 1 clique.

ALERTAS

- ☐ **13** Alerta no sintoma que o usuário sente (erro, latência), não em CPU a 80%.
- ☐ **14** Todo alerta é acionável, tem dono e link para o runbook.
- ☐ **15** Alerta baseado em SLO (taxa de consumo do error budget), não em limite chutado.
- ☐ **16** Revisão mensal dos alertas barulhentos: se ninguém age, apague ou ajuste.

Bug em minutos: alerta no sintoma → dashboard → trace → log com o mesmo trace_id → causa.

DASHBOARDS

- ☐ **17** Um dashboard por serviço com RED: taxa de requisições, erros e duração.
- ☐ **18** Deploys marcados no gráfico (anotação com versão e horário).
- ☐ **19** Infraestrutura com USE: utilização, saturação e erros de cada recurso.
- ☐ **20** A primeira tela responde em 10 segundos: está quebrado? Desde quando?

INCIDENTES

- ☐ **21** Runbook curto por alerta: o que olhar primeiro e como mitigar.
- ☐ **22** Canal e papéis definidos no incidente (quem comanda, quem comunica).
- ☐ **23** Mitigar antes de investigar: rollback ou feature flag primeiro.
- ☐ **24** Postmortem sem culpados, com ação, dono e prazo.

ANTES DE SUBIR UMA ROTA NOVA

- ☐ Log estruturado com request_id e trace_id
- ☐ Métrica de erro e latência p95 da rota
- ☐ Trace da rota até o banco e as chamadas externas
- ☐ Alerta no sintoma, com dono e runbook
- ☐ Dashboard do serviço atualizado
- ☐ Teste: force um erro e encontre a causa em 5 minutos

PARA IR ALÉM · SEGUE @LUCASADVICE

Observability primer — OpenTelemetry (em inglês):

opentelemetry.io/docs/concepts/observability-primer/

Traces — OpenTelemetry (em inglês): opentelemetry.io/docs/concepts/signals/traces/

Monitoring Distributed Systems: os 4 sinais de ouro — livro SRE do Google (em inglês):

sre.google/sre-book/monitoring-distributed-systems/

Alerting on SLOs — SRE Workbook do Google (em inglês): sre.google/workbook/alerting-on-slos/

Instrumentation e Alerting — boas práticas do Prometheus (em inglês):

prometheus.io/docs/practices/instrumentation/

Dashboard best practices (RED e USE) — Grafana (em inglês):

grafana.com/docs/grafana/latest/visualizations/dashboards/build-dashboards/best-practices/

Logging Cheat Sheet — OWASP (em inglês):

cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html

Postmortem Culture — livro SRE do Google (em inglês): sre.google/sre-book/postmortem-culture/