# INVESTIGAÇÃO DE INCIDENTES DE TI

Registro executivo • análise rRCI • preencher os campos destacados em azul nas demais abas

| Campo | Preenchimento | Orientações |
|---|---|---|
| ID do incidente | | Identificador no ITSM / GLPI / Jira |
| Título do incidente | | Sintoma principal e serviço afetado |
| Status | Em investigação | Aberto / Em investigação / Mitigado / Encerrado |
| Severidade | Alta | Crítica / Alta / Média / Baixa |
| Categoria | Infraestrutura | Infraestrutura / Rede / Segurança / Aplicação / Banco de dados / Nuvem / Mudança / Outro |
| Início do incidente | | Data e hora do primeiro impacto conhecido |
| Detecção | | Momento da identificação por monitoramento ou usuário |
| Restauração | | Data e hora do retorno do serviço |
| Encerramento | | Após validação de eficácia das ações |
| Serviço ou ativo impactado | | Hostname, aplicação, URL, conta de nuvem, segmento etc. |
| Responsável pela investigação | | Coordenador / facilitador |
| Equipe envolvida | | Áreas internas e fornecedores |
| Impacto no negócio | | Usuários, processos, operação, obrigações legais |
| Contenção imediata | | Medidas para estabilizar antes da análise definitiva |
| Causa raiz confirmada | | Referenciar evidências e aba 06 |

| Campo | Preenchimento | Orientações |
|---|---|---|
| Solução definitiva | | Correção técnica e mudanças no processo |
| Lições aprendidas | | Aprimoramentos na detecção e prevenção |

# DEFINIR O PROBLEMA

Método IS / IS NOT: delimitar com fatos o que ocorreu e o que ficou fora do escopo.

| Dimensão | É (IS) | Não é (IS NOT) | Diferenças relevantes / alterações |
|---|---|---|---|
| O quê? | Qual sistema, operação ou componente falhou? | Quais componentes similares não falharam? | Diferença de versões, dependências, configurações |
| Onde? | Em qual ambiente, local, VLAN, região AWS ou host? | Onde o comportamento não ocorre? | Topologia, disponibilidade zonal e roteamento |
| Quando? | Primeiro evento, duração, frequência e recorrência | Quando o problema não ocorreu? | Deploys, patches, alterações, backups, janelas |
| Extensão? | Quantos usuários, nós, requisições ou dados atingidos? | Quais usuários, regiões ou cargas não foram atingidos? | Qual a diferença de volume, carga ou perfil? |
| Sintomas | Erros, alertas, latência, indisponibilidade e comportamento | Sintomas investigados que não aparecem | Logs, traces e métricas para sustentar |
| Impacto | Perda operacional, serviços críticos, SLA/SLO, segurança | Processos preservados ou sem impacto | Evidências e fontes de medição |
| | | | |
| | | | |

# CRONOLOGIA DO INCIDENTE

Separar ocorrências observadas de interpretações; horários com fuso identificado.

| Data / hora | Evento observado | Origem / evidência | Ação / decisão | Responsável | Observações |
|---|---|---|---|---|---|
| | Primeiro sintoma ou alerta | | | | |
| | Confirmação e triagem | | | | |
| | Escalonamento e acionamento | | | | |
| | Contenção ou mitigação | | | | |
| | Serviço restaurado | | | | |
| | Validação pós-restauração | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# LEVANTAR CAUSAS POSSÍVEIS

Categorias equivalentes ao diagrama de Ishikawa, contextualizadas para infraestrutura e serviços de TI.

| Categoria | Hipótese / causa possível | Fatos que apoiam | Fatos que contradizem | Probabilidade | Próxima verificação |
|---|---|---|---|---|---|
| Tecnologia / máquinas | Hardware, storage, VM, container, processo, serviço | | | Não avaliada | |
| Métodos / processos | Mudança, deploy, documentação, execução e aprovação | | | Não avaliada | |
| Pessoas / equipes | Handoff, acesso, capacitação, comunicação e erro operacional | | | Não avaliada | |
| Medição / observabilidade | Alertas, logs insuficientes, ruído e falha de detecção | | | Não avaliada | |
| Materiais / dependências | Certificados, licenças, fornecedor, DNS externo, API e pacotes | | | Não avaliada | |
| Ambiente / contexto | Energia, rede, carga, capacidade, clima e infraestrutura física | | | Não avaliada | |
| Segurança / identidade | Autenticação, autorização, vulnerabilidade, malware e política | | | Não avaliada | |
| | | | | | |

# VALIDAR HIPÓTESES COM FATOS

Registrar como cada hipótese foi testada antes de declarar a causa raiz.

| ID da hipótese | Hipótese | Premissas necessárias | Teste / método | Evidência e referência | Resultado | Conclusão |
|---|---|---|---|---|---|---|
| H-01 | | | Consulta a syslog / journalctl / Event Viewer | | Pendente | |
| H-02 | | | Correlação entre mudança, alerta e métricas | | Pendente | |
| H-03 | | | Reprodução controlada em homologação | | Pendente | |
| H-04 | | | Comparação de configuração e versões | | Pendente | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

# COMPROVAR CAUSA RAIZ E PROPOR SOLUÇÃO

Usar os 5 porquês, evidência causal e análise de risco da mudança proposta.

| Etapa | Pergunta / elemento | Resposta / evidência | Responsável | Status |
|---|---|---|---|---|
| 5 porquês – 1 | Por que o incidente ocorreu? | | | Pendente |
| 5 porquês – 2 | Por que ocorreu a condição anterior? | | | Pendente |
| 5 porquês – 3 | Por que o controle anterior falhou? | | | Pendente |
| 5 porquês – 4 | Por que a organização não detectou / impediu? | | | Pendente |
| 5 porquês – 5 | Qual falha sistêmica permitiu o evento? | | | Pendente |
| Causa raiz | Enunciado claro, verificável e sem culpabilização | | | Pendente |
| Prova causal | Quais dados comprovam o vínculo entre causa e efeito? | | | Pendente |
| Correção | O que reestabelece o serviço? | | | Pendente |
| Ação corretiva | O que elimina a causa raiz identificada? | | | Pendente |
| Ação preventiva | O que evita casos semelhantes em outros ativos? | | | Pendente |
| Risco de implantação | A solução pode gerar regressão, indisponibilidade ou perda de dados? | | | Pendente |
| Rollback | Critérios, responsável e passos para reversão | | | Pendente |
| Monitoramento | Quais métricas / alertas atestam estabilidade? | | | Pendente |

# DIAGRAMA DE CAUSA E EFEITO – INSUMOS

Consolide categorias e hipóteses para montar o diagrama de Ishikawa em reunião de investigação.

| Categoria | Fator / possível causa | Evidência disponível | Status da hipótese |
|---|---|---|---|
| Infraestrutura / hardware | | | Pendente |
| Software / aplicação | | | Pendente |
| Rede / conectividade | | | Pendente |
| Procedimentos / mudanças | | | Pendente |
| Pessoas / organização | | | Pendente |
| Monitoramento / medição | | | Pendente |
| Fornecedores / dependências | | | Pendente |
| Segurança / identidade | | | Pendente |
| Ambiente físico / capacidade | | | Pendente |

# PLANO DE AÇÃO E ACOMPANHAMENTO

CAPA: correção, prevenção, detecção e validação da eficácia com responsável e prazo.

| ID | Tipo | Ação / entregável | Responsável | Prazo | Prioridade | Status | Evidência de conclusão | Eficácia validada? |
|---|---|---|---|---|---|---|---|---|
| A-01 | Contenção | Estabilizar ambiente e documentar intervenção | | | Crítica | Pendente | | Não |
| A-02 | Corretiva | Eliminar causa raiz comprovada | | | Alta | Pendente | | Não |
| A-03 | Preventiva | Aplicar correção / padrão a sistemas equivalentes | | | Alta | Pendente | | Não |
| A-04 | Detecção | Adicionar alerta, SLI/SLO ou teste automatizado | | | Média | Pendente | | Não |
| A-05 | Governança | Atualizar runbook, CMDB, baseline e change record | | | Média | Pendente | | Não |

| ID | Tipo | Ação / entregável | Responsável | Prazo | Prioridade | Status | Evidência de conclusão | Eficácia validada? |
|---|---|---|---|---|---|---|---|---|
| A-06 | Validação | Verificar ausência de recorrência no período definido | | | Alta | Pendente | | Não |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

# CHECKLIST DE ENCERRAMENTO E TRANSFERÊNCIA

O incidente somente deve ser encerrado após revisão das evidências e aceite do responsável pelo serviço.

| Critério de encerramento | Atendido? | Evidência / referência | Validador |
|---|---|---|---|
| Impacto e escopo do incidente documentados | Não | | |
| Cronologia consolidada com evidências e fontes | Não | | |
| Causa raiz confirmada por testes / correlação causal | Não | | |
| Contenção e restauração registradas | Não | | |
| Plano CAPA aprovado com proprietários e prazos | Não | | |
| Mudanças aprovadas conforme política organizacional | Não | | |
| Risco da solução e procedimento de rollback analisados | Não | | |
| Monitoramento e métricas de eficácia definidos | Não | | |
| Runbook, base de conhecimento e documentação atualizados | Não | | |
| Partes interessadas comunicadas e aceite registrado | Não | | |
| Eficácia das ações comprovada após período de observação | Não | | |

| Critério de encerramento | Atendido? | Evidência / referência | Validador |
|---|---|---|---|
| Lições aprendidas compartilhadas com a equipe | Não | | |

# PAINEL DE CONTROLE • INVESTIGAÇÃO DE INCIDENTE

Visão rápida dos registros e da execução do plano de ações; indicadores atualizados por fórmulas.

| Indicador | Valor | Interpretação |
|---|---|---|
| Ações cadastradas | (calculado na versão Excel) | Quantidade de linhas com ID no plano de ações |
| Ações concluídas | (calculado na versão Excel) | Quantidade de ações com status Concluída |
| Ações bloqueadas | (calculado na versão Excel) | Quantidade de ações com status Bloqueada |
| Ações pendentes | (calculado na versão Excel) | Quantidade de ações com status Pendente |
| Ações em andamento | (calculado na versão Excel) | Quantidade de ações com status Em andamento |
| Taxa de conclusão | (calculado na versão Excel) | Concluídas / total de ações |
| Hipóteses confirmadas | (calculado na versão Excel) | Quantidade de hipóteses confirmadas no levantamento |
| Itens de encerramento atendidos | (calculado na versão Excel) | Total de critérios com resposta Sim |

Observação: os indicadores automáticos e o acompanhamento completo das ações permanecem disponíveis na planilha Excel.