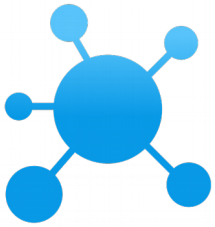
Universidade Federal de Viçosa
Diretoria de Tecnologia da Informação
Divisão de Apoio ao Usuário



Processo de Gestão de Incidentes

Fevereiro – 2016

HISTÓRICO DE ALTERAÇÕES

Data	Responsável	Observações
26/11/2015	Diego Fialho Rodrigues	Criação do documento
20/06/2016	Diego Fialho Rodrigues	Nova KPI (acúmulo de incidentes)
05/09/2017	Diego Fialho Rodrigues	Mudança de Indicadores

Sumário

1. INTRODUÇÃO

Um incidente pode ser definido como uma interrupção não planejada de um serviço de TI ou então uma redução em sua qualidade. Também pode ser considerado incidente uma falha de algum item de configuração que ainda não impactou o serviço do ponto de vista do usuário, por exemplo a falha de um disco que faz parte de um array RAID.

O processo de Gestão de Incidentes é responsável por gerenciar o ciclo de vida dos incidentes. O propósito de se gerenciar incidentes é fazer com que o serviço volte ao seu normal funcionamento o mais rápido possível minimizando impactos negativos no negócio e assegurando que os níveis de serviço acordados sejam atingidos.

Os objetivos do processo de gestão de incidentes são:

- Garantir que métodos padronizados serão usados para responder, analisar e documentar incidentes de forma eficiente e solícita.
- Aumentar a visibilidade e comunicação de incidentes entre os funcionários de TI.
- Melhorar a percepção do negócio em relação à TI através do uso de abordagens que resolvam e comuniquem rapidamente incidentes quando eles ocorrem.
- Alinhar as atividades e prioridades da Gestão de Incidentes com as necessidades do negócio.
- Manter a satisfação do usuário através da qualidade dos serviços de TI.

2. GATILHOS

Em uma visão mais purista, a ocorrência de falha em algum item de configuração é que disparará o processo de incidente. Contudo, o incidente precisa ser percebido e propriamente informado para que ações sejam tomadas. Isso pode acontecer de diversas maneiras. Através do gerenciamento de eventos, as ferramentas de monitoramento alertarão sempre que algo de anormal ocorrer. O incidente também poderá ser percebido por um de nossos funcionários e reportado. Através do usuário, o aviso de que algum serviço não está operando como deveria pode ocorrer por telefone, por e-mail e até presencialmente.

3. ATIVIDADES

As atividades do processo de Gerência de Incidentes serão definidas nas seções seguintes. O fluxograma pode ser visto na Figura 1.

3.1 Identificação e Registro do Incidente

Logicamente não se pode tomar nenhuma medida até que o incidente seja detectado. A percepção de que algo não vai bem pode acontecer de diversas formas como foi mostrado na seção de Gatilhos. Contudo, deve-se evitar ao máximo que o cliente entre em contato para relatar que sua unidade de negócio está sofrendo os impactos da inoperância do serviço. Um esforço deve ser feito para se detectar o incidente o mais cedo possível (geralmente com ferramentas de monitoramento de itens de configuração) para que a resolução aconteça o quanto antes.

O Zabbix será utilizado como principal ferramenta de monitoramento e alertará os responsáveis pelos serviços utilizando diferentes mídias (e-mail, chat, otrs). O Gerenciamento de

Eventos[1] terá uma relação próxima com o Gerenciamento de Incidentes no que diz respeito a tarefa de detectar eventos e classificá-los entre simples eventos ou incidentes. Ainda em relação a detecção de incidentes, não existe limitação para o uso de ferramentas. De acordo com necessidades específicas, poderemos usar scripts ad hoc para auxiliar na identificação de anormalidades nos serviços.

Todos os incidentes deverão ser registrados no OTRS. Mesmo os incidentes detectados automaticamente deverão se comunicar com o OTRS para abir um Chamado com as informações do incidente. O OTRS possui um módulo chamado System Monitoring que transforma e-mails de certos rementes em chamados. Basta configurar a ferramenta de monitoramento para enviar um e-mail informando o serviço afetado e que seu status atual é de incidente. Um chamado será aberto e tratado pelo Service Desk e os demais níveis de atendimento. O proprietário do chamado poderá registrar no OTRS todas os procedimentos tomados através de artigos. Quando o serviço for reestabelecido, a ferramenta de monitoramento deverá enviar outro e-mail informado que o status do serviço voltou a ser operacional. O OTRS irá automaticamente fechar o chamado.

Incidentes informados por clientes ou por técnicos podem ser abertos da forma convencional no OTRS (via fone ou e-mail). Como, inicialmente, não se tem uma classificação do tipo de chamado, o Service Desk ficará responsável por classificar o chamado entre Incidente, Requisição de Serviço, Requisição de Mudança, Evento, ou qualquer outro tipo de serviço que possa existir.

Entradas

- Monitoramento do Zabbix
- Reclamações de usuários
- Telefonemas de usuários
- Reclamações presenciais

Saídas

- Incidente registrado no OTRS.

3.2 Categorização do Incidente

Após o incidente ter sito registrado no OTRS, o Service Desk terá o papel de definir algumas informações em relação ao chamado:

- Identificar o cliente quando isto não for feito de forma automática.
- Definir se a origem do chamado é interna (monitoramento ou técnico da DTI) ou externa (cliente). Essa informação é importante para medirmos a capacidade de perceber os incidentes antes que o cliente o faça.
- Definir o Serviço afetado.
- Definir se houve impacto no negócio. Importante para medir a eficiência de soluções de alta disponibilidade, por exemplo.
- Relacionar o chamado com outros chamados referentes ao mesmo incidente. Por exemplo,

1 O Gerenciamento de Eventos ainda não foi implementado. Contudo o monitoramento dos serviços estão incrementalmente sendo configurados pelo Zabbix.

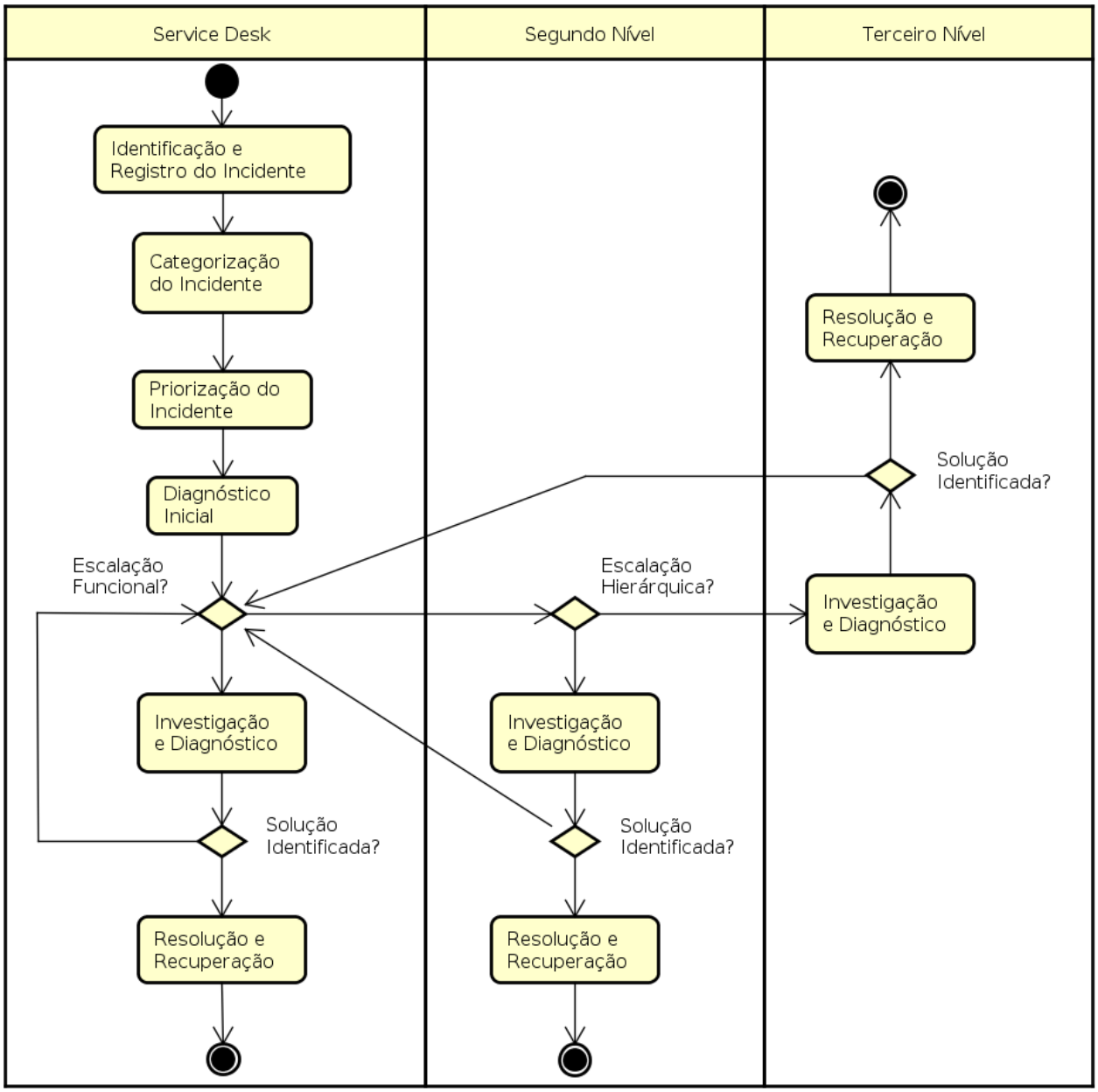


Figura 1: Fluxograma do Processo de Gerência de Incidentes.

vários clientes poderão ligar informando que não conseguem enviar e-mail (tratam-se de vários incidentes com a mesma causa e provavelmente com soluções parecidas).

- Relacionar o incidente com os itens de configuração afetados[2].
- Algumas vezes não será possível definir esses valores assim tão cedo no processo de gestão de incidentes. Por isso, o Service Desk ou qualquer outra divisão poderá definir ou alterar os valores à medida que o incidente vai sendo diagnosticado.

Entradas

- Incidentes similares
- Problema relacionado ao incidente
- Base de clientes

2 O OTRS não possui um módulo que armazena os itens de configuração e estes itens ainda estão sendo cadastrados.

- Catálogo de Serviços
- Base de Itens de Configuração

Saídas

- Incidente categorizado

3.3 Priorização do Incidente

Em um ambiente grande como a UFV, poderá haver vários incidentes abertos e teremos que decidir em qual trabalhar primeiro. Por isso, é importante definir níveis de prioridade aos incidentes para tratá-los com a devida urgência.

Geralmente a priorização pode ser feita em função de dois aspectos: a criticalidade do serviço e o seu impacto. A criticalidade se refere a importância do serviço para o negócio. O impacto pode ser definido pelo número de clientes afetados. Mas existem exceções. Por exemplo, um incidente poderá afetar apenas um cliente e ter impacto muito alto, como o serviço de folha de pagamento.

O OTRS utiliza uma matriz de criticalidade x impacto para definir a prioridade (Figura 2). A criticalidade é definida por serviço, de acordo com sua importância para o negócio. Este valor é definido nas fases de estratégia e de desenho de serviço.

IMPACTO / CRITICALIDADE	1 MUITO BAIXO	2 BAIXO	3 NORMAL	4 ALTO	5 MUITO ALTO
1 Muito Baixo	1 Muito Baixo	1 Muito Baixo	2 Baixo	2 Baixo	3 Normal
2 Baixo	1 Muito Baixo	2 Baixo	2 Baixo	3 Normal	4 Alto
3 Normal	2 Baixo	2 Baixo	3 Normal	4 Alto	4 Alto
4 Alto	2 Baixo	3 Normal	4 Alto	4 Alto	5 Muito Alto
5 Muito Alto	3 Normal	4 Alto	4 Alto	5 Muito Alto	5 Muito Alto

Figura 2: Matriz Impacto x Criticalidade.

O impacto é definido a cada chamado e, quando isso é feito, a prioridade é automaticamente preenchida de acordo com a matriz. Mesmo a prioridade sendo definida de forma automática, existe a possibilidade de mudar seu valor independente dos valores da matriz. Assim como a criticalidade, o impacto pode assumir valores de 1 (muito baixo) até 5 (muito alto). Segundo a ideia de classificação pelo número de pessoas afetadas, pode-se usar as seguintes regras para classificação de impacto:

- (1) Muito Baixo: afeta apenas um usuário.
- (2) Baixo: afeta um grupo pequeno de usuários.
- (3) Médio: afeta um departamento inteiro.
- (4) Alto: afeta uma região inteira da Universidade (um centro, por exemplo).
- (5) Muito Alto: Afeta toda a Universidade.

A SLA aplicada ao incidente poderá ser definida em função da prioridade.

Incidentes com priorização mais alta devem ter atenção imediata enquanto que os chamados

com priorização baixa possuem uma tolerância maior de prazo[3].

A prioridade também poderá mudar no ciclo de resolução do incidente. Algo que parecia ter impacto pequeno pode ter sua classificação alterada posteriormente pois ao se fazer um diagnóstico mais detalhado se descobriu que o impacto era muito maior, por exemplo. Por isso, o que foi definido no primeiro nível pelo Service Desk, pode e deve mudar em outros níveis.

Entradas

- Matriz Criticalidade x Impacto

Saídas

- Incidente priorizado

3.4 Diagnóstico Inicial

Caso o incidente tenha sido iniciado através de uma chamada telefônica, o Service Desk deverá realizar o diagnóstico inicial e, de preferência, resolver o incidente enquanto o usuário estiver na linha. Caso isto não seja possível, o Service Desk deverá informar ao usuário os próximos passos e informá-lo que atualizações serão enviadas por telefone ou por e-mail.

Quem fizer o diagnóstico inicial deverá lançar mão de ferramentas de monitoramento para verificar componentes que apresentam mal funcionamento e utilizar o FAQ do OTRS, que contém scripts que devem ser seguidos mediante certos sintomas. Obviamente o conjunto de scripts nunca será completo e deverá ser construído à medida que se toma conhecimento de novos tipos de incidentes.

Entradas

- FAQ incluindo soluções de contorno
- Zabbix

Saídas

- Decisão entre escalar ou não o incidente

3.5 Escalação do Incidente

Escalação Funcional

Quando o Service Desk decide que o chamado não pode ser resolvido por ele, o chamado deverá ser escalado para que outras equipes possam tratar o incidente.

Isso poderá ocorrer tanto pelo fato do Service Desk não ter condições de resolver a solicitação quanto pelo fato do prazo de primeiro atendimento estiver chegando em seu limite.

Antes de escalar, o Service Desk deverá fornecer informações do que já foi feito em notas explicativas ou por contato telefônico. O Service Desk deverá também monitorar o incidente

3 Precisamos implementar a Gestão de SLA e negociar prazos com as unidades de negócio.

(clicando no botão monitorar no OTRS) pois ele deverá acompanhar o andamento da resolução e manter o cliente informado.

O incidente deverá ser movido para a fila apropriada, geralmente subfilas das demais divisões (Filas N2). Uma vez que chamado foi movido, ele deverá ser tratado por um técnico. A política de alocação do chamado depende de cada divisão, em algumas o chefe designa o proprietário e em outras o próprio técnico aloca os chamados para si.

Escalação Hierárquica

Caso o incidente seja mais sério ou a equipe técnica não consiga resolver, ele deverá ser escalado a chefia da divisão. Isto é feito alocando o ticket para o chefe (mudando o proprietário) e avisando-o. O chefe então decidirá se será preciso envolver mais pessoas ou buscar ajuda externa para resolver o incidente.

3.6 Investigação e Diagnóstico

Nesta atividade, os responsáveis por tratar o incidente deverão fazer uma investigação mais profunda a fim de descobrir o que deu errado para então apresentar um diagnóstico. Todas as atividades deverão ser documentadas em forma de notas, inclusive as que fracassaram. Pode-se consultar o FAQ para obter informações de Erros Conhecidos e Soluções de Contorno.

Entradas

- FAQ incluindo soluções de contorno
- Zabbix

Saídas

- Incidente diagnosticado

3.7 Resolução e Recuperação

Quando uma possível solução é encontrada, ela deverá ser aplicada e testada. As ações a serem tomadas e as pessoas envolvidas podem variar muito dependendo do incidente. As ações devem ser devidamente documentadas no OTRS. Além disso, deve-se registrar as datas e horários de início da resolução e da recuperação. Esses valores são importantes para se saber o tempo gasto em cada estágio do incidente. Estes valores são armazenados nos campos adicionais ITSM do OTRS.

Neste ponto é importante ressaltar a diferença entre incidente e problema. O objetivo da resolução de incidentes é fazer com que o serviço volte a operar normalmente o mais rápido possível sem se preocupar com os motivos do incidente. A preocupação em descobrir as causas do incidente e prevenir sua recorrência fazem parte da gestão de problemas. Incidentes e problemas são dois conceitos correlatos, mas tratam-se de duas coisas diferentes por maior que sejam os impactos negativos no serviço.

Assim que o incidente for resolvido e o serviço volta a funcionar normalmente, o cliente

deverá ser devidamente informado. Em casos que sejam necessários testes por parte do usuário, deve-se aguardar um período antes de fechar o chamado (colocando o ticket em estado de pendente auto-fechamento).

Mais ou menos uma hora após o fechamento do chamado, é enviada uma pesquisa de satisfação ao cliente. Por isso, é importante evitar o fechamento de chamados sem ter certeza que os problemas foram sanados.

Todos os chamados possuem um campo de Revisão[4] indicando se o Service Desk já averiguou o atendimento. O objetivo é que se verifique todos os chamados após seu fechamento para saber se este foi corretamente categorizado e que todos os campos foram preenchidos. No caso de ausência de informações, o Service Desk ficará encarregado de entrar em contato com as pessoas que trabalharam no incidente para coletar as informações que estão faltando.

Caso o incidente envolva algum caso novo de erro conhecido ou algum script para resolução, deverá ser criado um novo chamado solicitando a criação do mesmo no FAQ. Posteriormente, a divisão responsável preparará o texto e inseri-lo na base de conhecimento.

Saídas

- Incidente resolvido

4. MATRIZ RACI

A matriz RACI (tabelas 1) relaciona os papéis desempenhados dentro de um processo com cada uma de suas atividades. Para cada relação existem quatro valores possíveis:

- R – Responsible: Representa quem irá, de fato, executar a tarefa. Deve haver ao menos um por tarefa.
- A – Accountable: Define quem será responsável pelo sucesso da atividade. Fica encarregado de verificar se a atividade foi realizada com sucesso e dentro do prazo. Deve haver um, e apenas um, por atividade.
- C – Consulted: Pessoas que serão consultadas durante a atividade. Geralmente exercem papel de conselho na tomada de decisões.
- I – Informed: Pessoas que deverão ser informadas da execução da atividade.

4 Criar o campo no OTRS.

Atividade	Service Desk	Segundo Nível	Chefias	Gerente de Incidentes
Identificação e Registro	A / R	R		
Categorização	A / R	C	C	C
Priorização	A / R	C	C	C
Diagnóstico	A / R	C	C	C
Escalação	A / R	R	R / C / I	C
Investigação	A / R	R / C	R / C / I	C
Recuperação	A / R	R / C	R / C /I	C

Tabela 1: Matriz RACI.

5. FATORES CRÍTICOS DE SUCESSO (CSF) E INDICADORES CHAVE DE PERFORMANCE (KPI)

5.1 Métricas Operacionais

ID	Nome	Possíveis Fontes
M1	Tempo médio para resolver incidentes de prioridade 1, 2 e 3	OTRS
M2	Número de Incidentes Registrados	OTRS
M3	Número de Incidentes de Prioridade 4 e 5 Registrados	OTRS
M4	Número de Incidentes Com Impacto no Negócio Registrados	OTRS
M5	Número de Serviços no Catálogo	Catálogo de Serviços
M6	Número de Dias do Período Reportado	
M7/	Número de Incidentes Resolvidos no período	OTRS
M8	Número de Incidentes Resolvidos no período dentro do Prazo	OTRS

Tabela 2: Métricas Operacionais.

5.2 Indicadores de Desempenho

ID	Nome	Cálculo	Alerta	Sucesso
KPI1	Tempo médio para resolver incidentes baixa prioridade	M1	< 3 dias	< 2 dias
KPI2	Número médio de Incidentes Registrados por serviço por dia	M2/(M5*M6)	< 0,5	< 0,2
KPI3	Número médio de Incidentes de Alta Prioridade Registrados por serviço por dia	M3/(M5*M6)	< 0,05	< 0,02
KPI4	Taxa de Resolução de Incidentes	M8/M7	> 80%	> 90%
KPI5	Taxa de Impacto no Cliente	M4/M2	< 30%	< 20%

Tabela 3: Indicadores de Desempenho.

5.3 Fatores Críticos de Sucesso

ID	Nome	Indicadores envolvidos
CSF1	Resolver Incidentes Rapidamente	KPI1
CSF2	Manter a qualidade dos Serviços de TI	KPI2, KPI3, KPI4,KPI5
CSF3	Manter a Satisfação do Usuário	KPI5

Tabela 4: Fatores Críticos de Sucesso.

6. OPORTUNIDADES DE MELHORIA DO PROCESSO

- Melhorar a categorização dos incidentes. Usa vários níveis de granularidade para saber os tipos de incidentes nas estatísticas? (ex. Localização → Serviço → Sistema → Aplicação). Ou então diferenciar a natureza do tipo de incidente (disponibilidade, capacidade, segurança).
- Medir o tempo gasto em cada etapa do incidente: detecção, diagnóstico, reparo, recuperação.
- Adição do campo “Resolução remota” no OTRS, para medir o volume de requisições resolvidas remotamente.
- Inserir CSF e/ou KPI’s para quantificar incidentes em relaçao à Itens de Configuração. O objetivo é verificar quais IC’s geram mais incidentes.