REO 8 – Gestão de Tecnologia da Informação

Exercitando o Gerenciamento de Incidentes

Pedro Antônio de Souza (201810557)

1. Definição de termos

Incidentes são os eventos que alteram o comportamento normal ou interrompem o serviço provido, como por exemplo: indisponibilidade de serviços ou problemas de permissionamento.

Problemas são os eventos causadores dos incidentes. Em geral, quando um problema é identificado ainda não se conhece sua causa. Portanto, o processo de gerenciamento de problema deve investigar a origem dos problemas.

Evento pode ser definido como qualquer acontecimento que tenha importância para o gerenciamento de TI. Os eventos podem ser categorizados naqueles que: (1) indicam uma operação regular, (2) indicam uma exceção e (3) indicam uma operação não usual, mas que não são uma exceção.

Acordo de Nível de Serviço (ANS) é o tratado firmado entre o prestador de serviços de TI e um cliente. Esse acordo descreve, em linguagem comum para ambas as partes, o serviço a ser prestado, as metas de nível de serviço e especifica as responsabilidades respectivas de cada parte.

2. Diferença entre Gerenciamento de Incidentes e Gerenciamento de Problemas

O **Gerenciamento de Incidentes** tem como objetivo solucionar incidentes, reportados ou encontrados pró-ativamente, a fim de restabelecer o serviço de TI aos usuários no menor tempo possível. Para isso, verifica-se na base conhecimento a documentação de ações para resolver o incidente de maneira rápida. É importante abrir um problema para um incidente (principalmente aqueles recorrentes) quando é desejado descobrir sua causa raiz.

Já o **Gerenciamento de Problemas** objetiva prevenir a ocorrência de incidentes e minimizar o impacto de incidentes inevitáveis. Para isso, pode-se analisar a predisposição

de um incidente ocorrer ou, como dito anteriormente, investigar a causa raiz de um incidente.

3. Atividades do Gerenciamento de Incidentes

Na imagem abaixo, pode-se observar o fluxo do gerenciamento de incidentes baseado no fluxo apresentado por Freitas (2013). As atividades principais estão em azul.

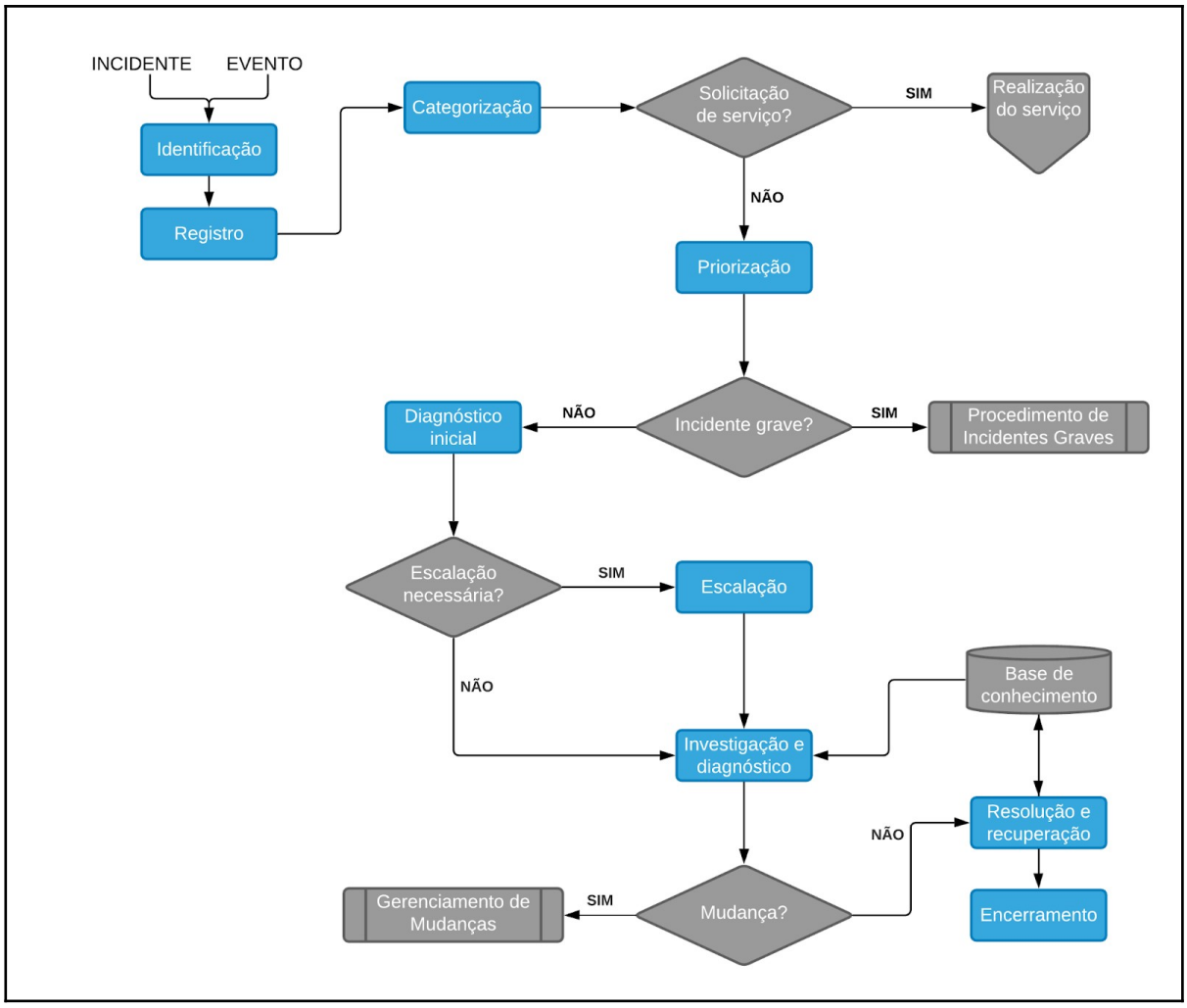

Figura 1 – Fluxo do gerenciamento de incidentes baseado no fluxo de Freitas (2013)

Ainda de acordo com Freitas (2013), as atividades do gerenciamento de incidentes podem ser descritas da seguinte forma:

- Na atividade de **identificação**, os incidentes são apontados por meio do gerenciamento de eventos, identificação pela equipe de TI ou por chamado realizado pelo usuário.
- Na atividade de **registro**, o incidente é armazenado em um sistema responsável pela sua catalogação e acompanhamento. O registro deve conter

todas as informações relevantes para atendimento do incidente e o histórico deve ser mantido para análises ou estudos futuros.

- Na atividade de **categorização**, os incidentes devem ser classificados de acordo com critérios preestabelecidos pela organização. O incidente deve ser encaminhado para a equipe correspondente à sua categoria.
- Na atividade de **priorização**, é definida em qual ordem os incidentes serão resolvidos. Para definir a prioridade, utiliza-se uma matriz de risco entre a urgência no tratamento do incidente e seu impacto na operação da empresa.
- Na atividade de **diagnóstico inicial**, como o próprio nome indica, é feita uma análise primária no incidente a fim de identificar o modelo de incidente. Para isso, pode-se consultar bases de conhecimento de incidentes anteriores para auxiliar no diagnóstico.
- Na atividade de **escalação**, o incidente é encaminhado para a equipe apta a tratá-lo.
- Na atividade de **investigação e diagnóstico**, busca-se identificar o que está fora da normalidade, entender a cronologia dos eventos que levaram ao incidente, identificar quais os eventos causaram o incidente, bem como analisar a base de conhecimento para identificar incidentes anteriores e conhecidos.
- Na atividade de **resolução e recuperação,** caso o incidente seja resolvido ou uma solução paliativa seja aplicada, deve-se avaliar se as ações tomadas devem ser registradas na base de conhecimento.
- Por fim, na atividade de **encerramento**, a central de serviços verifica se o incidente foi resolvido e se o usuário está satisfeito com a solução aplicada. Em caso positivo, o incidente é encerrado. Caso contrário, a central de serviços retorna o incidente para a equipe que o estava tratando.

4. Gerenciamento de incidentes pela DGTI/UFLA

Atualmente, a DGTI/UFLA dispõe do Plano de Gestão de Incidentes da Segurança da Informação e Privacidade[1] para definir princípios, conceitos, diretrizes e responsabilidades na gestão de incidentes.

Naquele documento, são definidos alguns canais para relatos de incidentes como telefones, e-mails e endereços, além de padronizar a forma como um incidente deve ser reportado.

O registro e catalogação dos incidentes é feito utilizando o software de registro de chamadas de suporte técnico GLPI[2].

O plano ainda define nove categorias em que os incidentes podem ser categorizados, três níveis de criticidade dos incidentes que são usados em sua priorização e seis status que auxiliam no acompanhamento do incidente.

A seção 14 daquele documento define alguns passos para a mitigação do incidente que possuem tarefas equivalentes às atividades "escalação", "investigação e diagnóstico", "resolução e recuperação" do gerenciamento de incidentes. Apesar desses passos serem mais detalhados do que o processo apresentado na Figura 1, não foi possível identificar uma etapa de "diagnóstico incial". Não se sabe o porquê da decisão de suprimir essa atividade, porém é importante lembrar que a análise prévia do incidente pode resultar em diminuição do tempo de resposta.

Por fim, é definido que, caso sejam necessárias, as recomendações devem ser feitas aos usuários, administradores de sistemas ou outras equipes de segurança no momento da finalização do incidente.

Uma boa prática adotada na DGTI/UFLA é a análise do incidente posterior ao seu fechamento. Assim, como o próprio documento define, é feita uma síntese das lições aprendidas para que sejam discutidos "erros e dificuldades encontradas na mitigação do evento ocorrido, propor melhoria na infraestrutura computacional e para os processos de resposta a incidentes".

1 https://dgti.ufla.br/images/politicas-e-normas/Plano_Gestao_Incidentes_v12_assinado.pdf

2 https://glpi.ufla.br

5. Dois possíveis indicadores para o gerenciamento de incidentes na DGTI/UFLA

O primeiro indicador sugerido é o **número de incidentes por tipo de notificação**, ou seja, se é uma notificação de incidente de privacidade de dados ou de segurança da informação (como é definido na seção 6 do Plano de Gestão de Incidentes da Segurança da Informação e Privacidade). Assim, pode-se perceber a recorrência de certos incidentes e identificar possíveis falhas ou ataques ao sistema.

O segundo indicador é o **número de incidentes por origem**. Todos os incidentes da DGTI/UFLA possuem a informação do indicador, já que é definido um padrão de notificação de incidentes. Com esse indicador é possível perceber áreas mais sensíveis à ocorrência de incidentes.

Referências

FREITAS, Marcos André dos Santos. **Fundamentos do Gerenciamento de Serviços de TI.** 2. ed. Rio de Janeiro: Brasport. 2013.