



Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins
Reitoria

PROCESSO DE GESTÃO DE INCIDENTES

1. INTRODUÇÃO

Segundo *Information Technology Infrastructure Library* (ITIL®), uma biblioteca de boas práticas em gerenciamento de serviços de TI, um incidente é a interrupção não planejada de um serviço de TI ou a redução da qualidade do serviço prestado (OGC, 2007). 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.

Existem vários tipos de incidentes envolvendo serviços de TI. Dentre eles podem ser citados: falta de acesso à internet, servidor fora do ar, mau funcionamento de computadores, ataques cibernéticos etc.

Dentro deste contexto, o processo de gestão de incidentes é responsável por gerenciar o ciclo de vida dos incidentes (UFV, 2016). Ele visa minimizar o impacto negativo que eles podem causar, reestabelecendo as operações o mais rápido possível. Este processo é realizado pela equipe de TI do IFTO e segue as boas práticas para gestão de TI do ITIL®.

1.1. Escopo

O propósito deste processo 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 qualidade de serviço acordados sejam atingidos. O processo de gestão de incidentes não inclui procedimentos detalhados para diagnosticar, investigar e resolver incidentes, mas pode fornecer técnicas para tornar a investigação e o diagnóstico mais eficientes. A investigação de incidentes mais severos geralmente requer conhecimento e experiência, em vez de etapas processuais.

1.2. Objetivos

O objetivo geral do processo de gestão de incidentes é restabelecer a operação normal do serviço de Tecnologia da Informação no qual ocorreu o incidente, o mais rápido possível, cumprindo o ANS. Neste sentido, este processo tem como objetivos específicos:

- a) Detalhar as características que determinam o modo de funcionamento do processo de gestão de incidentes, de maneira a assegurar que os benefícios esperados sejam alcançados, garantindo a qualidade dos serviços de TI e o menor impacto na ocorrência dos incidentes;
- b) Apontar indicador de desempenho que auxiliarão na tomada de decisão sobre quais serviços são necessários investimentos;
- c) Priorizar o atendimento dos incidentes relacionados aos serviços essenciais de TI;

- d) Escalonar os incidentes para os grupos de atendimento para que seja cumprido o prazo de resolução;
- e) Resolver os incidentes o mais rápido possível, restaurando a operação normal do serviço e minimizando os seus impactos adversos, nos processos de negócio. A operação normal é a entrega do serviço dentro das metas dos Acordos de Nível de Serviço no ambiente de TI do IFTO;
- f) Manter a comunicação dos status dos incidentes aos usuários dos serviços oferecidos pela TI;
- g) Garantir que métodos padronizados serão usados para responder, analisar e documentar incidentes de forma eficiente e solícita;
- h) Aumentar a visibilidade e comunicação de incidentes entre os funcionários de TI;
- i) Melhorar a percepção do negócio em relação à TI através do uso de abordagens que resolvam e comuniquem rapidamente incidentes quando eles ocorrem;
- j) Alinhar as atividades e prioridades da gestão de incidentes com as necessidades do negócio;
- k) Manter a satisfação do usuário através da qualidade dos serviços de TI.

1.3. **Abrangência**

O processo de gestão de incidentes aplica-se a todos os serviços que são prestados pela área de TI. Este processo abrange as atividades de identificação, registro, categorização, diagnóstico inicial, priorização, escalonamento, investigação e diagnóstico, resolução e recuperação e fechamento de incidentes envolvendo serviços prestados pela área de TI no âmbito do IFTO.

1.4. **Benefícios**

A execução eficiente do processo de gestão de incidentes traz os seguintes benefícios:

- a) Redução do impacto das indisponibilidades nos processos de negócio;
- b) Melhoria do índice de satisfação dos clientes de TI devido à redução do tempo de indisponibilidade (*downtime*) dos serviços de TI;
- c) Suporte ao cumprimento dos SLAs;
- d) Menor interrupção da equipe de suporte;
- e) Eliminação de incidentes perdidos ou não registrados;
- f) Maior confiabilidade dos serviços;
- g) Melhoria no relacionamento entre a TI e seus clientes;
- h) Redução dos custos no tratamento de incidentes;
- i) Monitoração aprimorada, onde permite que o desempenho confrontado com o Acordo de Nível de Serviço seja medido com mais precisão;
- j) Maior sensibilidade das necessidades dos clientes.

2. **DEFINIÇÕES**

Para melhor compreensão do processo de gestão de incidentes foram definidos os seguintes termos e conceitos:

- a) **Acordo de Nível de Serviço (ANS/SLA):** acordo entre um provedor de serviço de TI e o usuário. O acordo de nível de serviço descreve o serviço de TI, documenta metas de nível de serviço e especifica as responsabilidades do provedor de serviço de TI e do cliente;
- b) **Base de conhecimento:** um banco de dados lógico contendo dados e informações usadas pelo SGCS (Sistema de gerenciamento de conhecimento de serviço);
- c) **BDGC:** Banco de Dados de Gerenciamento de Configuração;
- d) **Central de serviços:** ponto único de contato entre o provedor de serviço e os usuários. Uma central de serviço típica gerencia incidentes, requisições de serviço e também a comunicação com os usuários. A Central de Serviços é primeiro nível na hierarquia dos grupos de suporte envolvidos na resolução de incidentes;
- e) **Escalonamento:** atividade que obtém recursos adicionais quando estes são necessários para atender o nível de serviço ou expectativas dos usuários. Existem dois tipos de escalonamento: Escalonamento funcional e Escalonamento hierárquico;
- f) **Evento:** qualquer mudança de estado que tenha significância para o gerenciamento de um serviço de TI ou outro item de configuração. O termo também pode ser usado para significar um alerta ou notificação criada por qualquer serviço de TI, Item de Configuração ou uma ferramenta de monitoramento. Os eventos normalmente exigem que o pessoal de operações de TI tome medidas e muitas vezes levam a incidentes, os quais devem ser registrados;
- g) **Gerenciamento de incidentes:** processo responsável pela gestão do ciclo de vida de todos os incidentes. Seu propósito é restaurar a operação normal do serviço de TI o mais rápido possível. A gestão de incidentes garante que a operação normal de um serviço seja restaurada tão rapidamente quanto possível e que o impacto no negócio seja minimizado;
- h) **Incidente:** interrupção não planejada (imprevista) de um serviço ou redução na qualidade de um serviço. Qualquer evento que cause ou possa causar uma interrupção ou uma redução da qualidade do serviço prestado;
- i) **Item de configuração (IC):** qualquer componente que necessite ser gerenciado para que possa entregar um Serviço de TI. Ex.: servidor, roteador, software, documentos, ap;
- j) **RDM:** requisição de mudança;
- k) **TMRS:** Tempo médio para recuperação de serviço.

3. GERENCIAMENTO DE INCIDENTES

Gerenciamento de incidentes é um processo que tem o objetivo de retomar um serviço o mais breve possível, causando o mínimo de danos ao negócio. Dessa forma, são mantidos os Acordos de Nível de Serviço firmados com as áreas de negócio. Isso pode ser feito através de um reparo rápido ou do fornecimento de uma solução alternativa ao cliente. O processo de gestão de incidentes utilizado pela para área de TI está detalhado na figura 1.

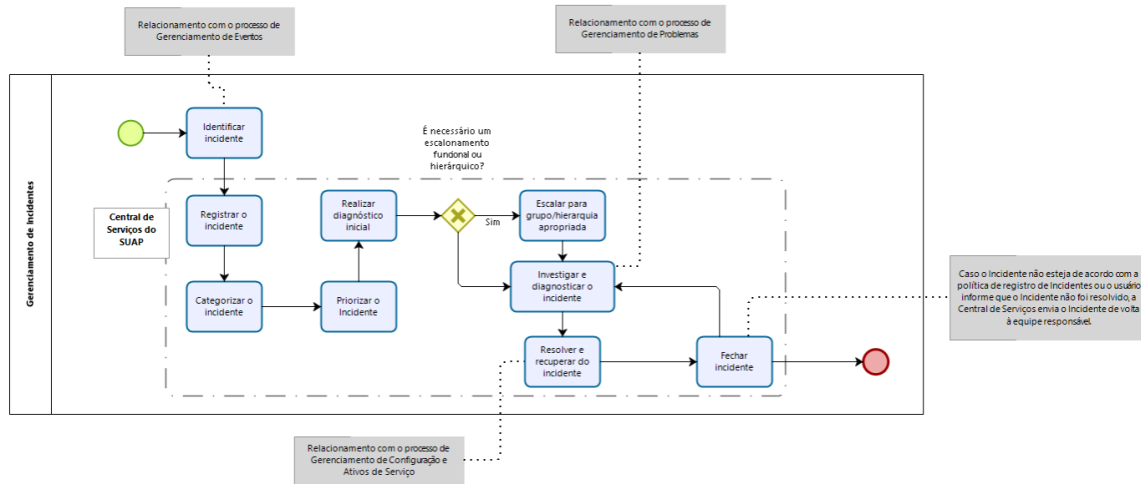


Figura 1 - Processo de gerenciamento de incidentes

O processo de gerenciamento de incidentes apresentado na figura 1 é executado pelas equipes de TI alocadas nas unidades do IFTO. Este processo é documentado através da central de serviços disponibilizada no SUAP. O processo apresentado na figura 1 é composto por 9 (nove) atividades, conforme apresenta a tabela 1.

Tabela 1 - Detalhamento do processo de gerenciamento de incidentes

<p>Entradas</p>	<ul style="list-style-type: none"> - Incidentes encaminhados pela central de serviços (SUAP). - Eventos encaminhados pelo gerenciamento de eventos. - Informações sobre os ICs do gerenciamento de configuração e ativos de serviço. - Informações sobre os níveis de serviços do gerenciamento de nível de serviço. - Informações sobre os serviços do gerenciamento de catálogo de serviço. - Informações sobre Mudanças do gerenciamento de mudanças. - Informações sobre erros conhecidos do gerenciamento de problemas. - Informações do sistema de gerenciamento de Conhecimento dos Serviços de TI. - <i>Feedback</i> de usuários dos serviços para o gerenciamento de relacionamento com o Negócio.
<p>Atividades</p>	<ol style="list-style-type: none"> 1. Identificar incidente. 2. Registrar incidente. 3. Categorizar incidente. 4. Priorizar o incidente. 5. Realizar diagnóstico inicial. 6. Escalar para grupo/hierarquia apropriada. 7. Investigar e diagnosticar o incidente. 8. Resolver e recuperar do incidente. 9. Fechar incidente.
<p>Saídas</p>	<ul style="list-style-type: none"> - Informações sobre incidentes para todos os outros processos. - Identificação de incidentes relacionados com itens de configuração. - Incidentes resolvidos para a central de serviços. - Abertura de registros de problemas. - Abertura de requisições de mudanças.

Fonte: Diretoria de Tecnologia da Informação

Segundo o processo apresentado na tabela 1, 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 servidores e estudantes e reportado. Através do usuário, o aviso de que algum serviço não está operando como deveria pode ocorrer pela central de serviços, telefone, e-mail e até presencialmente.

3.1. Identificar incidente

Atividade responsável por tomar ciência da ocorrência do incidente. Os incidentes podem ser identificados através de:

- a) Gerenciamento de eventos;
- b) Identificação da própria equipe de TI;
- c) Solicitação de atendimento de incidentes feita pelo usuário através de ligação telefônica, abertura de registro de incidentes via central de serviços (SUAP), ou qualquer outro canal de solicitação disponibilizado formalmente.

3.2. Registrar incidente

Atividade responsável por registrar os incidentes detectados no ambiente de TI do IFTO. Todos os incidentes devem ser registrados na central de serviços (SUAP), inclusive os chamados provenientes de ligações telefônicas.

Todas as informações relevantes para o atendimento do Incidente devem ser registradas e os históricos dos incidentes devem ser mantidos para posterior análise, se necessário. Essas informações podem incluir:

- a) Número de identificação único para o Incidente;
- b) Categoria do incidente de acordo com o tipo;
- c) Urgência do incidente;
- d) Impacto do incidente;
- e) Priorização do incidente;
- f) Data e hora de abertura, de cada atualização, resolução e fechamento;
- g) Identificação do técnico e grupo de suporte que está atendendo o Incidente;
- h) Fonte de origem do registro (e-mail, telefone, Intranet, etc.);
- i) Dados do solicitante com informações para contato;
- j) Descrição dos sintomas;
- k) Status do incidente (aberto, em atendimento, suspenso, resolvido e fechado);
- l) Item de configuração relacionado;
- m) Atividades realizadas para resolver o incidente;
- n) Resolução aplicada;
- o) Metas de atendimento do Acordo de Nível de Serviço.

3.3. Categorizar incidente

Atividade responsável por categorizar o tipo de incidente. Os incidentes devem ser categorizados adequadamente na central de serviços, em conformidade com o catálogo de serviços de TI.

Categorizar um chamado consiste em definir o tipo do chamado (p. ex. se é um incidente ou uma requisição) e o serviço do catálogo de serviços associado ao incidente. Os incidentes atualmente estão categorizados em: equipamentos, laboratórios de informática, redes e internet e sistemas e aplicativos.

Os incidentes podem ser classificados incidentes normais e graves. Incidente normal qualquer evento que possa causar impacto aos requisitos de negócio de um serviço de TI do IFTO. Inclui eventos que são comunicados diretamente pelos usuários ou gestores do IFTO por meio dos canais de atendimento existentes (telefone, e-mail e central de serviços) ou eventos identificados nas ferramentas de monitoração do ambiente.

Incidente grave são incidentes (conforme definição anterior) que ocorrem em serviços críticos do IFTO, conforme definido pelo catálogo de serviços. Alertam imediatamente o gerente do processo de incidentes.

3.4. **Priorizar o incidente**

Atividade responsável por definir uma ordem de atendimento dos incidentes de acordo com a urgência de tratamento e o impacto nas áreas de negócio. A priorização do incidente visa dar atendimento prioritário adequado aos incidentes.

Esta atividade utiliza critérios de qualidade para atender os requisitos do serviço definidos nos acordos de nível de serviço. Os incidentes deverão ser priorizados com base em uma classificação acordada com as partes interessadas para garantir que os incidentes com maior impacto no negócio sejam resolvidos de forma mais rápida.

Os incidentes de baixo impacto também devem ser gerenciados de forma eficiente para garantir que não consumam muitos recursos humanos e tecnológicos. No momento da resolução do incidente, o mesmo poderá ser escalado para fornecedores ou parceiros.

A prioridade identifica a importância relativa do incidente e é utilizada para identificar o tempo necessário para que as ações de tratamento sejam realizadas pelas equipes de suporte. Para determinar a prioridade, deve-se avaliar o impacto que o incidente causa e a sua urgência.

O impacto é uma medida do efeito do incidente no negócio. Ele normalmente baseia-se em como os níveis de serviços serão afetados. Vários fatores podem contribuir para a definição do nível de impacto, tais como número de usuários afetados e serviços envolvidos.

A urgência é a medida do tempo em que um incidente gerará impacto significativo no negócio, ou seja, o quão rápido o negócio precisa de uma resolução.

3.5. **Realizar diagnóstico inicial**

Atividade responsável por realizar o diagnóstico inicial e resolver o incidente o mais rápido possível, com os recursos de informação disponíveis, obedecendo os prazos de TMRS definidos no ANS. O diagnóstico inicial é feito por meio de perguntas e um roteiro de atendimento ou pela verificação dos sintomas informados, de forma a descobrir os sintomas e o real motivo do incidente.

O diagnóstico inicial refere-se à análise dos sintomas do incidente. O atendente deverá analisar todas as informações registradas no chamado a fim reproduzir ou diagnosticar o incidente de forma precisa. Ele poderá utilizar de várias meios que auxiliem na solução do incidente, dentre os quais, citam-se:

- a) Base de conhecimento e chamados semelhantes;
- b) Procedimentos e outros documentos técnicos da organização;
- c) Consulta a especialistas;
- d) Fornecedores externos.

Se existir um erro conhecido na base de conhecimento, o incidente deverá ser resolvido na central de serviços (SUAP). Caso contrário, deverá ser encaminhado imediatamente para o segundo nível de suporte.

Se com o diagnóstico inicial não for possível a resolução do incidente, este deverá ser escalado para o gerente do serviço. Porém, a função central de serviços é proprietária dos incidentes, com isto ela é responsável por monitorar e rastreá-los, durante seu ciclo de vida. Após a resolução, ela também é responsável pelo seu fechamento.

3.6. Escalar para grupo/hierarquia apropriada

Após o diagnóstico, se o técnico não conseguir aplicar a solução de contorno ou resolução, o incidente deve ser encaminhado para uma equipe capaz de resolver o incidente. É importante que o atendente da central de serviços se certifique de que o chamado possui as informações suficientes para o atendimento. Caso o chamado não possua informações suficientes para o atendimento, a central de serviços deve solicitar mais informações ao usuário, utilizando o SUAP ou através do telefone.

Antes de escalar, o atendente deverá fornecer informações do que já foi feito em notas explicativas ou por contato telefônico. Caso o incidente seja mais sério ou a equipe técnica não consiga resolver, ele deverá ser escalado para outro nível de atendimento. O atendente então decidirá se será preciso envolver mais pessoas ou buscar ajuda externa para resolver o incidente.

3.7. Investigar e diagnosticar o incidente

Atividade responsável identificar uma solução de contorno ou resolução para o incidente fins restabelecer o serviço à operação normal. Investigar e diagnosticar o incidente busca e registra as possíveis causas e direciona para uma solução definitiva ou temporária.

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. Esta atividade consiste nas seguintes tarefas de:

- a) Identificar o que está fora da operação padrão de um serviço;
- b) Entender a cronologia dos eventos que levaram ao incidente;
- c) Confirmar as informações que levem à classificação de priorização;
- d) Identificar os eventos que podem ter iniciado o incidente;
- e) Analisar informações do sistema de gerenciamento de conhecimento de serviço para identificar incidentes anteriores, registros de problemas, base de erros conhecidos, informações de fornecedores, eventos ou requisições de mudanças.

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. Se após esgotados os recursos funcionais, o objetivo dessa atividade não puder ser cumprido, deve ser aberto um registro de problema e realizar escalação hierárquica.

3.8. Resolver e recuperar do incidente

Atividade responsável por aplicar solução encontrada no subprocesso de investigação e diagnóstico e gerar entrada para outros processos relacionados à solução. Esta

atividade pode ser realizada tanto pela central de serviços quanto pelo suporte de 2 nível. Em ambos casos o atendente deverá atuar na resolução do incidente conforme solução descrita na base de erros conhecidos e registrar, no histórico do chamado, as ações realizadas.

Na resolução de incidentes são considerados os níveis de serviços especificados em acordos com as áreas de negócio. Para a resolução de incidentes deve-se verificar se há solução cadastrada nas bases de conhecimento sobre erros conhecidos e problemas.

Assim que o incidente for resolvido e o serviço voltar a funcionar normalmente, o solicitante deverá ser devidamente informado. Em casos que sejam necessários testes por parte do usuário, deve-se aguardar um período antes de fechar o chamado. Para a resolução do incidente deverão ser observados:

- a) Se for identificada uma solução de contorno ou resolução para o incidente, deve ser avaliado se essa solução altera os atributos de itens de configuração;
- b) Se esse tipo de alteração for escopo do gerenciamento de mudanças, deverá ser aberta uma Requisição de Mudança (RDM) para resolução da falha;
- c) Se esta solução pode ser aplicada sem a necessidade de abertura de RDM, a solução é aplicada, o registro de incidente é atualizado e os incidentes são encaminhados para a central de serviços para fechamento do incidente.

As ações a serem tomadas e as pessoas envolvidas podem variar muito dependendo do incidente. As ações devem ser devidamente documentadas. 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.

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.

3.8.1. Níveis de serviços

A área de TI tem dois níveis de atendimento:

- a) **Suporte nível 1:** equipe de execução de procedimentos técnicos de baixo risco e impacto, em serviços não críticos, com baixo conhecimento técnico. São especialistas destinados a avaliar, planejar e monitorar a gestão de incidentes para a sua organização funcional e plataforma tecnológica específica. Funcionam como elo de ligação entre os diferentes departamentos, a fim de que haja um processo específico bem definido de ações. Atende os usuários através da central de serviços (SUAP). Realiza a classificação dos incidentes de acordo com o catálogo de serviços, executando a complementação das informações junto ao usuário, sempre que necessário. Realiza o diagnóstico inicial dos incidentes e executa os procedimentos de solução que são pré-aprovados, baixo risco e impacto, de acordo com o catálogo de serviços. Muitas vezes é caracterizada pela equipe que realiza o atendimento presencial para a solução dos incidentes.
- b) **Suporte nível 2:** equipe de execução de procedimentos de médio e alto risco e impacto, em quaisquer serviços, com alto conhecimento técnico. É o tipo de suporte técnico mais aprofundado do que o nível 1. O pessoal de suporte de nível 2 pode ser mais experiente ou conhecedor de um determinado produto ou serviço. Além disso, o nível 2 pode fornecer solução de problemas especializados. Departamentos especializados (Sistemas, Redes e Suporte Técnico) fornecerão suporte nível 2 em suas respectivas áreas de especialização. Elabora procedimentos de solução para incidentes graves, problemas e/ou mudanças. Executa atendimentos em serviços críticos (alto impacto e risco) de acordo com o catálogo de serviços.

3.9. Fechar incidente

Atividade responsável por verificar se o incidente foi realmente resolvido e a satisfação do usuário. O encerramento de incidentes pode ser promovido em três situações:

- a) Desistência ou confirmação de solução do incidente por parte da pessoa que o registrou;
- b) Prazo para manifestação da satisfação com o atendimento expirado;
- c) O gerente do processo de incidentes pode considerar o incidente improcedente encerrando o mesmo com o devido parecer.

Os objetivos específicos desta atividade são:

- a) Confirmar o restabelecimento da operação normal do serviço;
- b) Encerrar o registro do chamado na ferramenta;
- c) Obter o *feedback* do usuário quanto a resolução do atendimento.

O usuário deve ser informado sobre o encerramento do chamado. Caso o incidente não esteja de acordo com a política de registro de incidentes ou o usuário informe que o incidente não foi resolvido, o atendente deverá através da central de serviços atender novamente o incidente.

4. PAPÉIS E RESPONSABILIDADES

Um papel é um conjunto de responsabilidades, atividades e autoridades definidas em um processo e atribuídas a uma pessoa, equipe ou função. Os papéis e responsabilidades dos envolvidos no processo de gestão de incidentes são:

4.1. Dono do processo

Profissional com perfil de gestão e autoridade funcional instituída para alocar recursos, bem como definir a visão e os objetivos de negócio do processo. No IFTO este papel é realizado pela Diretoria de Tecnologia da Informação que tem as seguintes responsabilidades:

- a) Garantir que o processo seja adequado ao propósito do IFTO;
- b) Deliberar acerca da visão e os objetivos de negócio do processo;
- c) Realizar as melhorias necessárias no processo;
- d) Deliberar acerca da alocação de recursos no processo;
- e) Garantir que a documentação do processo esteja atualizada e acessível a todos os envolvidos;
- f) Garantir que os envolvidos sejam informados das mudanças efetuadas no processo;
- g) Garantir que relatórios com os indicadores de desempenho sejam produzidos e distribuídos entre os interessados;
- h) Desenhar modelos de incidentes e fluxo de trabalho para o tratamento de incidentes;
- i) Trabalhar junto com outros donos de processo para garantir que uma abordagem integrada esteja sendo adotada para a gestão de incidentes;

- j) Garantir que os envolvidos recebam os treinamentos adequados para a fiel execução do processo.

4.2. Gerente do processo

Profissional com experiência em gerenciamento e coordenação de equipes. No IFTO este papel é representado pelas coordenações de TI.

- a) Indicar pessoas adequadas aos papéis definidos no processo;
- b) Prover relatórios sobre os incidentes dos serviços de TI do IFTO;
- c) Administrar impasses durante a execução do processo;
- d) Aferir os indicadores de desempenho do processo de incidentes;
- e) Gerenciar as equipes de atendimento de incidentes.
- f) Monitorar as atividades do gerenciamento de incidentes e propor melhorias para o processo.
- g) Coordenar as interfaces entre o gerenciamento de incidentes e os outros processos, especialmente eventos e problemas.
- h) Desenvolver procedimentos e políticas de modelos de incidentes, escalação, priorização e resolução de conflitos no atendimento de incidentes.
- i) Registrar e informar ao dono do processo as sugestões de melhorias no processo e sistema de gerenciamento de serviços;
- j) Garantir que os usuários sejam mantidos informados sobre seus incidentes;
- k) Decidir sobre a alocação de incidentes aos atendentes de incidentes;
- l) Decidir sobre as escalações hierárquicas de incidentes;
- m) Garantir a inclusão e atualização dos erros conhecidos na base de conhecimento;
- n) Auxiliar os atendentes na solução de incidentes;
- o) Elaborar e divulgar relatórios de desempenho da execução do processo de incidentes.

4.3. Gerente do serviço

Cada gerente de serviço de TI possui as responsabilidades abaixo elencadas, relativas aos incidentes ocorridos nos seus respectivos serviços:

- a) Elaborar relatórios de incidentes;
- b) Monitorar as atividades de gerenciamento de incidentes;
- c) Desenvolver procedimentos e políticas de modelos de incidentes, escalação, priorização e resolução de conflitos para o atendimento de incidentes.

4.4. Equipe de TI

A equipe de gestão de incidentes referentes à área de TI é representada por analistas e técnicos de TI, tendo como responsabilidade:

- a) Resolver e recuperar incidentes;

4.5. **Atendente**

Papel desempenhado por analistas e técnicos de TI. Tem as seguintes responsabilidades:

- a) Entrar em contato com o solicitante sempre que for identificada a ausência de informações necessárias para o atendimento dos incidentes;
- b) Realizar a categorização dos incidentes no prazo acordado no SLA;
- c) Fornecer feedback técnico a respeito das atividades, riscos e viabilidade dos incidentes sempre que julgar necessário;
- d) Escalonar os incidentes para os demais níveis de atendimento;
- e) Executar o atendimento dos incidentes de acordo com os procedimentos documentados no catálogo de serviços da respectiva classificação do incidente;
- f) Recategorizar os chamados categorizados de forma equivocada e comunicar os operadores da central sobre o equívoco;
- g) Solucionar os incidentes que não possuem solução documentada na base de conhecimento ou que não foram solucionado pela central de serviços no prazo definido pelo ANS;
- h) Atualizar ou adicionar novos registros de erros conhecidos na base de conhecimento;
- i) Solucionar incidente.

4.6. **Solicitante**

Pessoa responsável por identificar e registrar o incidente, tendo como responsabilidades:

- a) Identificar o incidente;
- b) Registrar o incidente;
- c) Fechar o incidente.

5. **MATRIZ RACI**

A matriz RACI apresentada na tabela 2 é um método utilizado para definir com clareza os papéis e responsabilidades de cada ator na execução da atividade relacionada ao processo. A sigla RACI significa, em inglês: *Responsible, Accountable, Consulted e Informed*.

- a) **Responsible (Responsável):** pessoa, função ou unidade organizacional responsável pela execução de uma atividade no âmbito de um processo; representa quem irá, de fato executar a tarefa. Deve haver ao menos um por tarefa;
- b) **Accountable (Responsabilizado):** dono da atividade, deverá fornecer os meios para que a atividade possa ser executada, e será responsabilizado caso a atividade não alcance os seus objetivos; cada atividade só pode possuir um 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 (Consultado):** pessoa que deve ser consultada durante a execução da atividade; As informações levantadas junto a essas pessoas tornam-se entradas para a execução da atividade; Geralmente exercem papel de conselho na tomada de decisões;

d) **Informed (Informado):** pessoa que será informada acerca do progresso da execução da atividade.

Tabela 2 - Matriz de responsabilidades

Atividade	DP	GP	GS	ETI	S	A
Identificar incidente.	I	I	I	A	R	I
Registrar incidente.	I	I	I	A	R	I
Categorizar incidente.	C	C	I	C	I	A/R
Priorizar o incidente.	C	C	C	C	I	A/R
Realizar diagnóstico inicial.	C	C	C	R	I	A/R
Escalar para grupo/hierarquia apropriada.	C/I	C/I	R	C/I	I	A/R
Investigar e diagnosticar o incidente.	C/I	C/I	C	C/I	I	A/R
Resolver e recuperar do incidente.	C/I	C/I	C	C/I	I	A/R
Fechar incidente.	I	I	I	I	I	A/R
Avaliar atendimento.	I	I	I	I	A/R	I
Reabrir incidente.	I	I	I	I	A/R	I

Legenda:

DP: Dono do Processo (Diretoria de TI).

GP: Gerente do Processo (Coordenações de TI).

GS: Gerente do Serviço (Responsável pelo serviço)

ETI: Equipe de Gestão de Incidentes.

S: Solicitante.

A: Atendente.

6. INDICADOR DE DESEMPENHO

O processo de gestão de incidentes deverá ser monitorado e constantemente medido através de indicadores de desempenho. Em geral, o papel responsável por coletar os dados do indicador é o dono do processo. No entanto, havendo um responsável diferente, então o mesmo deve ser informado.

Esse monitoramento tem como objetivo acompanhar a eficácia do processo, identificando tendências, falhas e oportunidades de correções, promovendo sempre a melhoria contínua. A tabela 3 apresenta as métricas que foram definidas para o processo de gestão de incidentes.

Tabela 3 - Indicadores de desempenho

Indicador	01 - Número de incidentes abertos.
Descrição	Apresentar a quantidade de incidentes abertos.
Objetivo	Apresentar a quantidade de chamados referentes à incidentes que foram abertos.
Periodicidade	Mensal
Fórmula	Soma de chamados de incidentes abertos.
Meta	Diminuir a quantidade de incidentes abertos.
Fonte	SUAP

Ferramenta	SUAP
Responsável	Coordenação de Suporte e Manutenção.

Indicador	02 - Número de chamados fechados.
Descrição	Apresentar a quantidade de incidentes fechados.
Objetivo	Apresentar a quantidade de incidentes que foram fechados.
Periodicidade	Mensal
Fórmula	Soma de chamados de incidentes fechados.
Meta	Aumentar a quantidade de incidentes fechados.
Fonte	SUAP
Ferramenta	SUAP
Responsável	Coordenação de Suporte e Manutenção.

Indicador	03 - Média de tempo de atendimento dos chamados (horas).
Descrição	Apresentar a média de tempo de atendimento dos chamados realizados pelo solicitante durante o mês.
Objetivo	Apresentar a média de tempo de atendimento referente ao mês.
Periodicidade	Mensal
Fórmula	Média
Meta	Diminuir a média do tempo de atendimento dos chamados no mês.
Fonte	SUAP
Ferramenta	SUAP
Responsável	Coordenação de Suporte e Manutenção

Indicador	04 - Média de tempo de resposta dos chamados (horas).
Descrição	Apresentar a média de tempo de resposta para incidentes que foram resolvidos durante o mês.
Objetivo	Apresentar a média de tempo de resposta referente ao mês.
Periodicidade	Mensal
Fórmula	Média
Meta	Diminuir a média de tempo de resposta dos chamados (incidentes) atendidos durante o mês.
Fonte	SUAP
Ferramenta	SUAP
Responsável	Coordenação de Suporte e Manutenção.

7. 7. PROCESSOS RELACIONADOS

O processo de gestão de incidentes de serviços de TI está relacionado com os seguintes processos:

- a) **Gerenciamento de problema:** processo que investiga e resolve a causa-raiz dos incidentes, para prevenir ou reduzir o impacto da recorrência com erros conhecidos e soluções de contorno para restaurar o serviço rapidamente;
- b) **Gerenciamento de catálogo de serviços:** processo responsável por criar e manter o catálogo de serviços e por garantir que esteja disponível àqueles autorizados a acessá-lo.;
- c) **Gerenciamento de nível de Serviço:** processo responsável por definir, acordar, registrar e gerenciar níveis de serviços;

- d) **Gerenciamento de mudanças:** processo responsável por garantir que métodos e procedimentos padronizados sejam utilizados para avaliar, aprovar, implementar e revisar todas as mudanças na infraestrutura e desenvolvimento de TI de maneira eficiente, a fim de minimizar o impacto relacionado aos serviços e usuários;
- e) **Gerenciamento de eventos:** processo responsável por monitorar e gerar alertas ou notificações de um serviço de TI ou item de Configuração considerados relevantes para os processos de gerenciamento de serviços de TI e para cumprimento dos ANS;
- f) **Gerenciamento de configuração e ativos de serviços:** processo responsável por fornecer os dados usados para identificar e atender aos incidentes. Possibilita a identificação do item com defeito e ajuda na avaliação do impacto de um incidente.

8. PRÁTICAS RECOMENDADAS

Para que o processo de gestão de incidentes seja executado com sucesso são definidas as seguintes regras:

8.1. Identificação e registro

A identificação de um incidente é caracterizada pela interrupção não planejada de um serviço de TI ou uma redução na qualidade desse serviço. A identificação de incidentes tem natureza reativa e deve fazer parte do cotidiano de toda a operação de serviços. Neste sentido, devem ser observadas as seguintes práticas:

- a) Todos os incidentes devem ser registrados, inclusive os incidentes reportados. Esse registro deve conter informações precisas e detalhadas em relação ao incidente ocorrido;
- b) Cada incidente deve ser registrado e gerenciado para garantir que seja resolvido em um momento que atenda às expectativas do usuário. Os incidentes podem ser identificados pelos seguintes meios listados: central de serviços, e-mail e ferramenta de monitoração. O gerente do processo deve apoiar e fornecer insumos processuais para toda operação;
- c) As informações sobre incidentes devem ser armazenadas em registros de incidentes em uma ferramenta adequada. Idealmente, essa ferramenta também deve fornecer links para itens de configuração (ICs) relacionados, alterações, problemas, erros conhecidos e outros conhecimentos para permitir um diagnóstico e recuperação rápidos e eficientes;
- d) A central de serviços deve solicitar mais informações do usuário quando o chamado não dispuser de informação suficiente para o atendimento;
- e) Ações corretivas, preventivas e oportunidade de melhorias no processo devem ser registradas e encaminhadas ao dono do processo. O banco de dados de erros conhecidos deve ser atualizado constantemente;
- f) Os incidentes devem possuir códigos de status para identificar em que ponto se encontram no seu ciclo de vida. São exemplos de status:
- **Aberto:** incidente registrado, mas que ainda não foi associado a um profissional de suporte para resolução.
 - **Em atendimento:** incidente sendo investigado e resolvido.
 - **Suspensão:** aguardando resolução de pendência (por parte do solicitante) para dar andamento ao atendimento.
 - **Resolvido:** foi aplicada uma resolução para o incidente e a operação normal foi restaurada, mas ainda não foi validada pelo usuário.
 - **Fechado:** a restauração normal foi restaurada e o usuário validou a resolução do incidente.

g) Incidentes podem ser reabertos sempre que o usuário apontar falhas no serviço. Como prerrogativa, o incidente só pode ser reaberto pelo mesmo usuário solicitante ou afetado que apontou a falha inicialmente. 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;

h) 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.

8.2. **Categorização**

Na categorização dos incidentes devem ser observadas as seguintes práticas:

- a) Os chamados devem ser categorizados e priorizados pela central de serviços (SUAP), dentro do prazo acordado;
- b) Incidentes devem ser resolvidos e documentados na central de serviços (SUAP).

8.3. **Priorização**

Para atendimento dos incidentes são definidos níveis de prioridade para tratá-los com a devida urgência. A priorização dos incidentes pode ocorrer por três diferentes meios:

- a) Pela categorização definida no acordo de nível de serviço, de acordo com o catálogo de serviços;
- b) Intervenção do gerente do processo;
- c) Matriz entre impacto e 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.

Os incidentes de maior prioridade terão precedência no atendimento. A priorização é definida com base em uma matriz de risco entre a urgência do tratamento do incidente e o impacto que o incidente causa nas áreas de negócio. O impacto pode ser definido de acordo com alguns dos critérios a seguir:

- d) Quantidade de áreas de negócio afetadas;
- e) Quantidade de serviços impactados;
- f) Nível de exposição da imagem institucional;
- g) Risco de perdas financeiras;
- h) Conformidade com leis e regulamentações.

A priorização poderá ser realizada pela matriz de impacto e urgência levando em consideração tendências, conforme apresenta a figura 2. Gravidade é o parâmetro que avalia o impacto. A urgência é a determinação do tempo máximo que a instituição pode suportar esses impactos sem solução. A tendência avalia o agravamento do incidente. De acordo com os valores obtidos na gravidade, urgência e tendência a prioridade será definida.

Gravidade (impacto)	Urgência (prazo)	Tendência (agravamento)	Prioridade
Muito Alto	Imediata	Piora imediata	1
Alto	Urgência média	Piora rápida	2
Médio	Urgência baixa	Piora lenta	3
Baixo	Atendimento normal	Piora muito lenta	4
Muito Baixo	Pode aguardar	Piora estagnada	5

Figura 2 - Matriz GUT de priorização.

A prioridade do incidente conforme demonstrada na figura 2 é determinada pela pontuação obtida após avaliação do seu impacto e da sua urgência e tendência. Para a análise do impacto, são utilizados dois fatores:

- i) **Usuários afetados:** avalia o número de usuários afetados ou se é um usuário que possui atendimento especial;
- j) **Serviços envolvidos:** avalia a criticidade do serviço para o negócio.

Para avaliar a gravidade são definidas as seguintes prioridades:

- (1) Muito Alto: afeta todo o IFTO;
- (2) Alto: afeta um campus do IFTO;
- (3) Médio: afeta um setor inteiro;
- (4) Baixo: afeta um grupo pequeno de usuários;
- (5) Muito baixo: afeta apenas um usuário.

Como resultado da escala de priorização, um acordo de nível de serviço pode definir, por exemplo, que os serviços devem ser atendidos de acordo com a seguinte escala de metas de atendimento de prioridade:

- Prioridade (1): TMRS = 2 horas.
- Prioridade (2): TMRS = 4 horas.
- Prioridade (3): TMRS = 1 dia útil.
- Prioridade (4): TMRS = 3 dias úteis.
- Prioridade (5): TMRS = 5 dias úteis.

Os prazos definidos na prioridade devem estar refletidos nos prazos de atendimento. Se, por exemplo, foi definido no prazo de atendimento que a central de serviços e o gerenciamento de incidentes somente operam em horário comercial de segunda à sexta-feira, então os prazos são os seguintes:

- Prioridade (1): TMRS = 2 horas.
- Prioridade (2): TMRS = 4 horas.
- Prioridade (3): TMRS = 1 dia útil.
- Prioridade (4): TMRS = 3 dias úteis.
- Prioridade (5): TMRS = 5 dias úteis.

Em função de conflitos hierárquicos por “entendimentos” de prioridade por parte dos clientes, gerentes e a equipe de TI, é recomendado que sejam identificados os clientes VIP (*Very Important Person*) da instituição. Esses usuários podem ter níveis de priorização diferenciados em relação aos usuários comuns dos serviços de TI, como por exemplo um setor que possui um serviço crítico para instituição.

Tem prioridade máxima para atendimento, os incidentes considerados graves. Estes incidentes causam grande impacto e exigem máxima urgência de atendimento. Assim, são os incidentes de maior prioridade possível e por este motivo demandam procedimentos excepcionais para atendimento. Um incidente pode ser considerado grave se:

- k) Afeta um ou mais serviços críticos para os processos de negócio do IFTO, durante períodos especificados nos Acordos de Nível de Serviço. O catálogo de serviços possui a informação de quais serviços são críticos;
- l) Produz impacto significativo na reputação, conformidade legal ou regulatória, segurança física, pessoal ou de informação confidencial. Neste caso, é necessário que o gerente do processo declare o incidente como grave;
- m) O gerente do processo de incidentes pode declarar qualquer incidente como grave. Ele tem autonomia para isso.

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 pela central de serviços, pode e deve mudar em outros níveis.

8.4. Escalonamento

A escalção assegura que o atendimento seja eficiente. Antes de escalar, o atendente deverá fornecer informações do que já foi feito em notas explicativas ou por contato telefônico.

Estes procedimentos só podem ser interrompidos com autorização do gerente do processo de incidentes. Os cenários de escalção e alerta poderão ser configurados de acordo com a necessidade dos gestores de cada nível de atendimento.

Devido às diferentes prioridades e diversos incidentes em tratamento ao mesmo tempo, é preciso estar atento para evitar que o prazo de atendimento acordado seja ameaçado por um esquecimento ou falha de comunicação. Para escalar um incidente relacionado ao serviço de TI deverá ser utilizado dois tipos de escalções:

- a) **Escalção Funcional:** escalção para equipe com capacidade para resolver o Incidente. Geralmente são equipes especializadas com mais experiência e perfis de acesso dos serviços diferenciados das equipes de níveis inferiores. Requer acordos de nível operacional entre as equipes para garantir o atendimento do acordo de nível de serviço. Exemplo: equipe nível 1 de suporte a desktop, equipe nível 2 de suporte à rede, de suporte especializado a sistemas e aplicações;
- b) **Escalção Hierárquica:** Incidentes que requerem ações de resolução mais complicadas, como aquisição de recursos adicionais, acionamento de fornecedores, se previamente definido no Acordo de Nível de Serviço, para a devida tomada de decisão sobre os melhores procedimentos de resolução do incidente. Outro tipo muito comum de Escalção Hierárquica é a resolução de conflitos no atendimento de incidentes sobre prioridades de atendimento de incidentes com a mesma classificação. Supondo que há três incidentes na fila de atendimento com classificação de prioridade 2, o gerente do processo de incidentes poderá ser acionado para definir a ordem de atendimento dos incidentes com mesma classificação de prioridade. Caso o incidente seja mais sério ou a equipe técnica não consiga resolver, ele deverá ser escalado para o gerente do processo. Este ator decidirá se será preciso envolver mais pessoas ou buscar ajuda externa para resolver o incidente.

8.5. Diagnóstico e Resolução

Para o diagnóstico e resolução dos incidentes devem ser observadas as seguintes práticas:

a) Os incidentes podem ser diagnosticados e resolvidos por pessoas em muitos grupos diferentes, dependendo da complexidade do problema ou do tipo de incidente. Os incidentes devem ser identificados pela equipe de TI, por sistemas de monitoramento ou, então, relatados pelos usuários;

b) Grande parte dos incidentes serão resolvidos pela central de serviços (SUAP). Incidentes mais complexos geralmente serão encaminhados para uma equipe de suporte para resolução. Normalmente, o roteamento é baseado na categoria de incidente, o que ajuda a identificar a equipe correta.

8.6. Monitoramento, controle e documentação

Para o monitoramento, controle e documentação de incidentes devem ser observadas as seguintes práticas:

a) Os incidentes relacionados à serviços de TI devem ser monitorados e documentados periodicamente de forma que possibilite a melhoria contínua do processo. Esta atividade deverá ser realizada uma vez ao ano. Eventuais ajustes a serem realizados deverão ser registrados para possibilitar o aprendizado colaborativo;

b) As ferramentas de gerência de redes deverão monitorar e alertar os responsáveis pelos serviços utilizando diferentes mídias. O gerenciamento de eventos deverá 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.

c) Ainda em relação a detecção de incidentes, não existe limitação para o uso de ferramentas. De acordo com necessidades específicas, poderão ser utilizados scripts ad hoc para auxiliar na identificação de anormalidades nos serviços.

9. REFERÊNCIAS

Office of Government Commerce (OGC, 2007). **ITIL: The Official Introduction to the ITIL Service Lifecycle**. London: TSO (The Stationary Office), 2007. ISBN 9780113310616. Disponível em: <<https://www.kornev-online.net/ITIL/The%20Official%20Introduction%20to%20the%20ITIL%20Service%20Lifecycle.pdf>>. Acesso em: 10 jan. 2021.

Palmas, 12 de janeiro de 2021.

Kleyton Matos Moreira

Diretor de Tecnologia da Informação

Paula Karini Dias Ferreira Amorim

Presidente do Comitê Gestor de Tecnologia da Informação
PORTARIA Nº 242/2019/REI/IFTO, DE 28 DE FEVEREIRO DE 2019



Documento assinado eletronicamente por **Kleyton Matos Moreira, Diretor**, em 16/04/2021, às 09:42, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Paula Karini Dias Ferreira Amorim, Presidente**, em 16/04/2021, às 11:04, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site http://sei.iftto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1274201** e o código CRC **F52C7CBB**.

Avenida Joaquim Teotônio Segurado, Quadra 202 Sul, ACSU-SE 20, Conjunto 1, Lote 8 - Plano Diretor Sul — CEP 77020-450 Palmas/TO — (63) 3229-2200
portal.iftto.edu.br — reitoria@iftto.edu.br

Referência: Processo nº 23235.000413/2021-79

SEI nº 1274201