Modelo para sistema de gestão da atividade de um Network Operations Center

Projeto Final de Licenciatura

Elaborado por:
Yan Henrique Rocha Sant'ana- nº de aluno: 20192410

Orientador(es):
Virgínia Araújo

Barcarena
Novembro de 2022

O autor é o único responsável pelas ideias expressas neste relatório.

Agradecimentos

Aproveito para deixar uma palavra de agradecimento para todos que estiveram e me ajudaram durante a minha caminhada.

Quero agradecer, em primeiro lugar, a Deus, que me permitiu continuar com força e energia para chegar até o último ano com capacidade. Em segundo lugar, aos meus pais, que me deram as condições iniciais para seguir na carreira académica, e que me ajudaram nos diversos tópicos, dando forças para seguir. Em terceiro lugar, a minha professora-orientadora, Virgínia Araújo, que me auxiliou a dar forma a este trabalho, pela confiança de estruturar o trabalho, e pelo constante esclarecimento de dúvidas. Em quarto lugar, à minha namorada, Amanda Chaves, que foi e é o meu porto-seguro psicológico e emocional durante todo este tempo, tudo seria bem mais difícil sem ela, o dia seguinte é muito mais calmo sabendo que você está comigo. Obrigado pela constante confiança e sinceridade, pelos dias incontáveis de suporte.

Obrigado também a todos os meus amigos, que me orientaram em ideias, mas também foram um importante suporte emocional durante esta trajetória.

Todos tiveram um papel fundamental para chegar neste dia, obrigado a todos.

Resumo

Um dos componentes vitais para a estruturação e manutenção de Internet Service Providers (ISPs) é possuir um Network Operations Center (NOC) eficiente e coeso. O trabalho tem como objetivo propor um modelo para um sistema de gestão da atividade de um NOC, para que haja maior eficiência processual e analítica, aliado com a intervenção dos operadores. No contexto organizacional observado, através da revisão da literatura e de um questionário aplicado aos colaboradores da organização, é possível observar que a equipa do NOC realiza múltiplas tarefas simultâneas, e grande parcela dessas ocupações, trata-se de incidentes de menor impacto e reincidentes, o que aumenta a sobrecarga de trabalho e consequentemente, prejudica o tratamento e resolução de incidentes de maior impacto. Com a estruturação do modelo proposto, por meio de processos ITIL, concluiu-se que, uma possível solução para o problema identificado era a capacidade de automatizar processualmente, toda a criação e resolução de incidentes de menor impacto. A solução proposta assenta-se através do Postman REST API para a integração da plataforma do ITSM (BMC Remedy) e da plataforma que dispõe a alarmística enviada pelos equipamentos de rede, já utilizada pela organização em questão, TEOCO Fault Management Software, e assim, realizar a criação e finalização de tickets para registo dos incidentes, através do estado da alarmística. As conclusões que são apresentadas cumprem com o objetivo proposto, o que permite o direcionamento do NOC para incidentes que possuem maior importância; garante uma transparência do estado da rede pela organização; aumenta a eficiência e eficácia na resolução de incidentes; além de escalabilidade, apresentados nos trabalhos futuros do projeto.

Palavras-chave: Network Operations Center; NOC; ITSM; REST API.

Abstract

One of the vital components for structuring and maintaining Internet Service Providers (ISPs) is having an efficient and cohesive Network Operations Center (NOC). The objective of this thesis to propose a model for a system for managing the activity of a NOC, so that there is greater procedural and analytical efficiency, combined with the intervention of operators working in the NOC. In the organizational context observed, through a literature review and a questionnaire applied to the organization's employees, it is possible to observe that the NOC performs multiple simultaneous tasks and a large portion of these occupations are incidents of lesser impact and repeated incidents, which increases the work overload and consequently, impairs the treatment and resolution of incidents of greater impact. Structuring the model with the ITIL processes, it was concluded that a possible solution to the identified problem was the ability to procedurally automate all the creation and resolution of lower impact incidents. The proposed solution is based on the Postman REST API for the integration of the ITSM platform (BMC Remedy) and the platform that sent the alarms by the network equipment, already used by the reviewed organization (TEOCO Fault Management Software) and thus, create and finalize tickets to record the incidents through the alarm status. The presented conclusions comply with the proposed objective, and therefore allows the NOC to focus in the incidents that are of greater importance; ensures transparency of the state of the network by the organization; increases efficiency and effectiveness in incident resolution; and adds scalability, presented in the future works of the project.

Keywords: Network Operations Center; NOC; ITSM; REST API.

Índice

Lista de Abreviaturas e Siglas

NOC – Network Operations Center

BTS – Base Transceiver Station

RSSI – Received Signal Strength Indication

ISP – Internet Service Provider

CMDB – Configuration Management Database

CI – Configuration Item

IA – Inteligência Artificial

API – Application Program Interface

JSON – JavaScript Object Notation

HTML – HyperText Markup Language

Índice de Figuras

Índice de Tabelas

1 Introdução

Este projeto final de curso assenta-se na construção de uma proposta de solução para automatismo de incidentes de menor impacto em um NOC (Network Operations Center). Será descrito os processos necessários para o seu desenvolvimento, bem como os conceitos para compreensão do leitor. A proposta de solução não será efetivamente desenvolvida, mas sim, estruturada mediante todos os seus processos.

1.1 Contexto e motivação

Em um ambiente organizacional, para melhoria de processos, e consequentemente, melhora do desempenho, foi sugerido a implementação de automatismos no departamento do NOC (Network Operations Center). O NOC é uma centralização de equipas de rede, que realizam a sua supervisão e a saúde da rede, é a primeira linha de serviço quando há alguma falha na entrega do serviço, como uma falha de energia em um Datacenter, cortes de fibra, falhas no sistema de resfriamento, ou seja, tudo que esteja relacionado com quebras de serviço, o NOC é o primeiro atuante na sua resolução. Basicamente todo ISP (Internet Service Provider) possui um Network Operations Center, para gerir, supervisionar, monitorar e analisar o tráfego de toda a sua rede, seja a rede móvel, por voz, por fibras, e solucionar os seus incidentes.

A supervisão ocorre por meio de alarmísticas disponibilizadas por meio de uma plataforma integradora de alarmes. Cada equipamento de transmissão dispõe de alarmísticas, que são transferidas para a plataforma integradora, e o supervisor do equipamento realiza as ações necessárias. Os alarmes são transferidos por meio de *thresholds* definidos previamente, e uma vez que o equipamento não cumpre os devidos requisitos, é enviado para o supervisor, um alarme com as informações necessárias, por exemplo, uma BTS (Base Transceiver Station) está com o seu RSSI (Received Signal Strength Indication) abaixo do indicado, é enviado instantaneamente, um alarme com as informações do equipamento naquele momento.

Contudo, a partir do momento que o alarme é enviado, o técnico que faz parte do NOC irá analisar minuciosamente a informação e consequentemente, tomar as ações necessárias, e caso não consiga solucionar, enviará para o suporte de segunda linha ou para a verificação do técnico no terreno. A partir do envio do alarme, não há mais nenhum processo automatizado que realiza

a análise e tomada de decisão, são ações completamente humanas, e para a diminuição dos erros, há a proposição do automatismo como o suporte nos Network Operations Center.

1.2 Descrição do problema

Em ISPs, no qual o seu principal serviço é a disponibilização da rede, é intrínseco a composição de um forte e resiliente departamento do Network Operations Center, para uma boa análise inicial dos primeiros incidentes, para evitar que se escalem. O NOC realiza diversas atividades simultâneas, como suporte especializado para técnicos no terreno, tratamento de requisições das 2ª linhas, além do tratamento e monitorização dos incidentes de rede. Com o aumento da quantidade de serviço entregue com o passar dos anos, e nenhuma inovação à nível processual, o NOC analisado não consegue cumprir com as suas principais tarefas de monitoramento e otimização da rede, o que diminui o desempenho e a entrega do serviço. A proposta busca diminuir a atuação do operador do NOC em incidentes reincidentes sem impacto para o utilizador final da rede, permitindo que o técnico do NOC seja capaz de garantir a qualidade na entrega do serviço final com maior eficiência.

1.3 Objetivos

Este projeto tem como objetivo, propor um modelo para um sistema de gestão da atividade de um NOC, para que haja maior eficiência processual e analítica, aliado com a intervenção dos operadores. Conforme indicado anteriormente, o NOC analisado apresenta constante crescimento na quantidade de entrega de serviço, contudo, não houve evolução à nível processual para garantir uma qualidade na análise de desempenho e gestão de falhas. O principal objetivo é garantir com que haja uma maior eficácia de processos, através de um modelo de gestão para incidentes reincidentes e sem impacto. O modelo proposto, por meio da alarmística enviada pelos equipamentos de rede, irá documentar os incidentes e encaminhar a sua resolução de forma automática, sem intervenção do técnico, e assim, garantir uma maior eficiência processual e analítica. Outro objetivo da proposta de solução é permitir que haja uma maior perceção para os incidentes de maior impacto e a melhoria na capacidade de gestão. Ao eliminar uma grande parcela de serviço do técnico do NOC no tratamento de incidentes de menor impacto, busca-se direcionar o foco para incidentes que possui um maior impacto no serviço final, para que o seu diagnóstico e resolução sejam eficazes, além de garantir uma melhor gestão durante o tratamento do incidente. Desta forma, o modelo de gestão procura

certificar uma maior qualidade na entrega do serviço, estabelecendo padrões processuais e permitindo o direcionamento do NOC para incidentes de maior relevância.

2 Revisão da Literatura

Durante este capítulo, são revistos os tópicos intrínsecos para a compreensão do modelo, bem como os conceitos, processos e aplicações.

2.1 Eficiência do Network Operation Center (NOC)

O *Network Operations Center* é uma forma de integração e monitoramento de rede, que dispõem de uma série de alarmísticas que, além de transmitir o funcionamento dos equipamentos presentes na rede, busca garantir o melhor nível de *Quality Of Service* (QoS) possível. O NOC assenta-se através do "Fault Management", gestão de falhas na entrega do serviço, identificada por meio da alarmística enviada pelos equipamentos de rede, para assim, desenvolver as suas três funções essenciais: deteção, diagnóstico e remediar (solucionar).

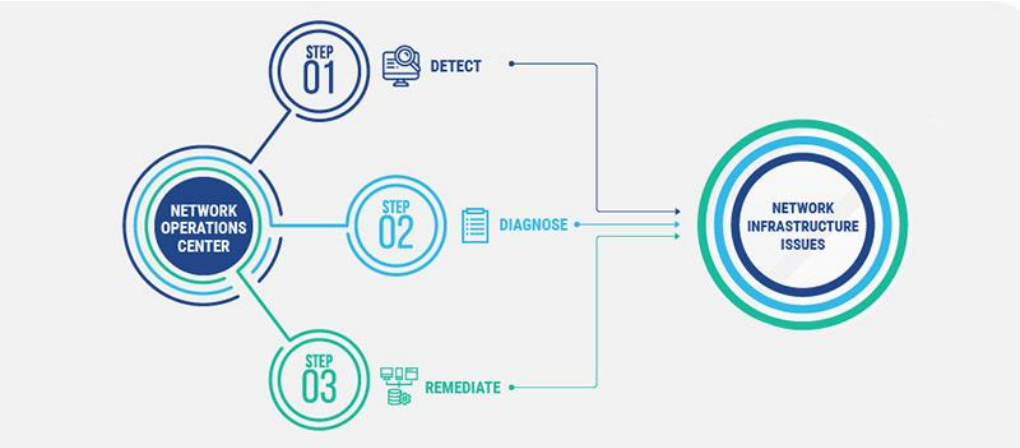


Figura 1: *Workflow de um operador do NOC. - retirado de: https://www.extnoc.com/network-operations-center/*

Com o auxílio da Figura 1, temos as três principais funções de um operador de um Network Operation Center. A Figura 2 exemplifica a disposição de alarmísticas de rede ao operador NOC, por meio do monitoramento das alarmísticas compartilhadas pelos equipamentos de rede há a deteção de todo tipo de incidente que acontece, por exemplo, caso uma antena que faz o serviço de redes móveis (BTS) fique sem serviço, um conjunto de alarmes são enviados para o operador, esse é a parte de "deteção". Posteriormente, o operador NOC realiza o "diagnóstico" da situação: ainda no mesmo exemplo, com a alarmística enviada pela antena sem serviço, o

operador realizará as devidas análises de forma a tentar evidenciar o incidente. Suponhamos que, antes da antena ficar sem serviço, apresente alarmes de falhas de energia, logo, poderá ser uma avaria geral na rede elétrica pelo fornecedor de energia. Identificado o motivo, o colaborador dirige-se para o último tópico: "remediar". Com a recolha de todas as informações, serão tomadas as atitudes necessárias para corrigir a situação, seja o acionamento de equipas técnicas para avaliar a situação no terreno, ou até mesmo a ajuda da segunda linha – equipa de suporte para o NOC -, de forma a auxiliar, tanto na resolução, como no diagnóstico da situação.

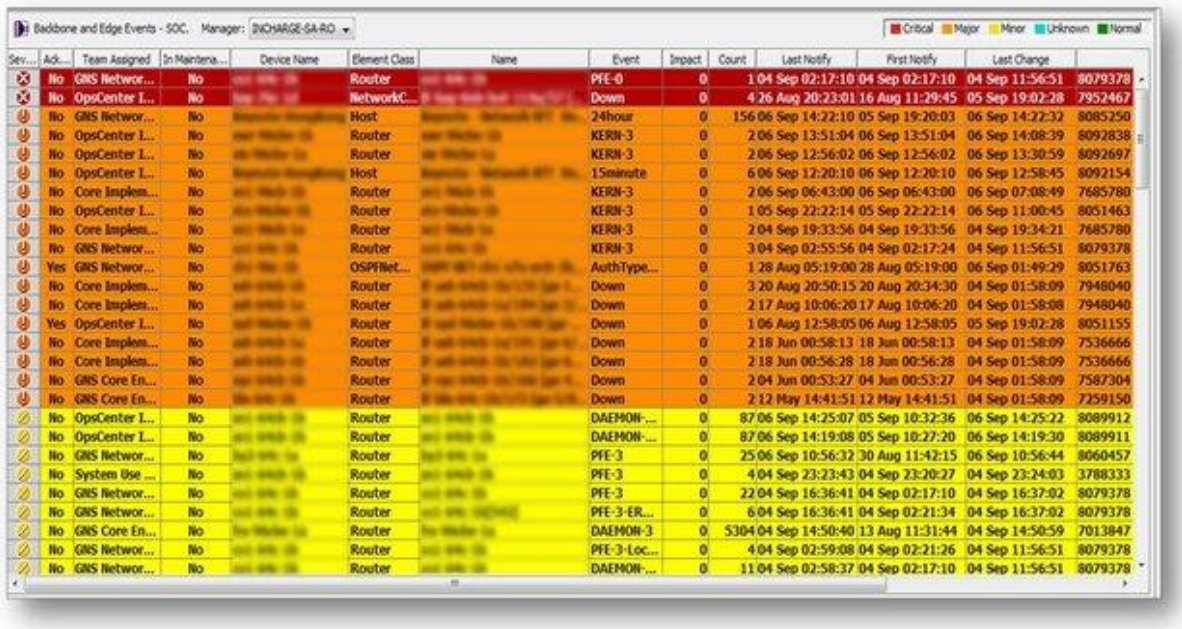


Figura 2: *Exemplo de alarmísticas dispostas para o operador do NOC. - retirado de: https://www.researchgate.net/publication/221519030_CueT_Human-Guided_Fast_and_Accurate_Network_Alarm_Triage/figures*

Esses foram somente três tópicos essenciais realizados por um operador de um Network Operations Center para solucionar uma avaria na rede, contudo, uma função determinante para uma boa execução do trabalho é a documentação das ações. Suportadas por uma plataforma de ITSM (IT Service Management), há uma interligação entre os principais serviços IT de uma organização. Ainda com o exemplo da antena sem serviço: suponha que há um cliente móvel que utilizará da antena móvel que, entretanto, ficou sem operação. O consumidor poderá ligar ao serviço ao cliente, a questionar sobre a razão do serviço não estar com a mesma qualidade. Com a interligação pelo ITSM, o serviço ao cliente poderá notificar o utilizador da avaria no

local, indicando a sua previsão de resolução, mas para isso, o processo deve ser bem documentado.

A eficiência do NOC é vital para o decorrer de resoluções de incidentes dentro de uma organização, principalmente em ISPs (Internet Service Provider). Em questionários realizados em 2001, na Lucent Technology (empresa de telecomunições americana, atual Alcatel-Lucent), mostram que o NOC é visto como o componente mais crítico de suas operações, com 85% de participação nas respostas, representado na figura 3.

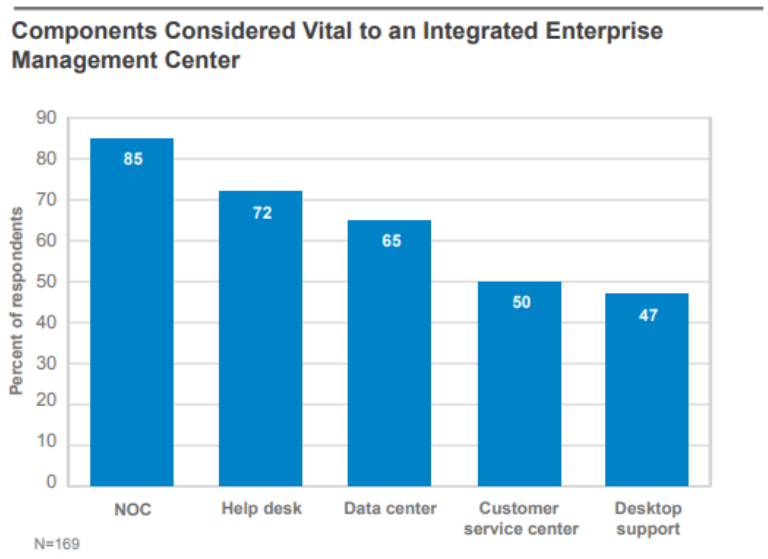


Figura 3: *Componentes considerados vitais para um Centro de Gestão Empresarial Integrada. - retirado de: "Network Operations Centers" (Lucent Technologies, 2001)*

"Essencialmente, o NOC tem a função de garantir o serviço por meio do cumprimento de SLAs, apesar de equilibrar com os custos de operação do ISP. O NOC coleta monitoramento de performance (SNMP, ping, traceroute) e alarmes, que podem ser registados como tickets." (A. Mohammed, et.al, 2021). Ou seja, o NOC é vital para o cumprimento a nível de serviço, para aumentar a QoS (Quality of Service), mas também a nível operacionais, conforme citado anteriormente.

Além disso, é importante citar que o trabalho efetuado por um operador NOC transcende o tratamento de alarmística, mas também atua como suporte para técnicos que realizam trabalhos no terreno, solicitações enviadas por email, como por exemplo, análises da 2ª linha que implicam atuação no terreno. São todos trabalhos realizados pelo NOC, e dessa forma, para

propor uma melhor eficiência e tratamento de incidentes de redes, que foi proposta esta solução. Com um serviço com tamanha vitalidade e importância para uma organização, é intrínseco que haja uma construção de uma plataforma que permita a integração da rede, e por fim, uma melhora processual.

2.2 Gestão de Serviço (ITSM)

Visando maior resiliência na organização, foram estipulados padrões e frameworks para auxiliar a Gestão de Serviço. Cada plataforma garante um âmbito de gestão, por exemplo, COBIT (Control Objectives for Information and Related Technologies) uma framework criada pela ISACA (Information Systems Audit and Control Association) e garante que profissionais governem e giram a TI de forma holística, incorporando todas as áreas funcionais de negócios e de TI de ponta a ponta. Contudo, para o acompanhamento do Network Operations Center, é imperioso uma plataforma de gestão de serviço que esteja direcionada para a constante modificação do estado dos seus ativos, através do ITSM (IT Service Management).

ITSM é definido pela Universidade de Berkeley como "uma estrutura de gestão de TI baseada em processos destinada a alinhar a entrega de serviços de TI com as necessidades de nossos clientes." Essa estrutura, por sua vez, está diretamente estruturada pelos processos ITIL (Information Technology Infrastructure Library) um conjunto de boas práticas usadas por empresas e outras entidades para gerir os seus serviços de TI.

Inicialmente, para uma boa gestão de serviços IT, é imperioso que haja uma criação de um catálogo de todo tipo de ativos, para que assim possa documentar todo tipo de impacto. Esta categorização fica registada em uma CMDB (Configuration Management Database), onde cada componente é registado como um CI (Configuration Item), e por sua vez, cada CI tem o seu grau de importância, o responsável, e toda informação que seja relevante, como, por exemplo, o seu fornecedor, como definido pela AXELOS (2020)

É de responsabilidade do NOC participar na gestão de incidentes. O trabalho da gestão de incidentes foca a resolução deste incidente de acordo como seu grau de criticidade, de forma a recuperar a acordada qualidade de serviço. O operador do NOC, através da alarmística apresentada, tem primeiramente a responsabilidade de avaliar se cada alarme identifica realmente um incidente. Se assim for, garante que seja criado um registo, e preparar a

documentação para a sua resolução. Caso esteja fora do seu alcance, será criado uma tarefa, endereçada para a equipa para tratar da recuperação do serviço, por exemplo, a 2ª linha para suporte ou uma equipa parceira para validação no terreno.

"Incidente é uma interrupção ou redução da qualidade do serviço." (AXELOS, 2020). A prática de Gestão de Incidentes permite que as interrupções ou degradações de serviço sejam reduzidas, com foco na identificação rápida dos incidentes e a reposição do serviço no seu estado acordado. Em um ISP, há diversos tipos de falhas/incidentes que dificultam na entrega do serviço, sendo estes:

- Falha de energia em equipamentos de rede;
- Ataques de negação de serviço (DDoS);
- Quebras de links de rede;
- Cortes de fibra óptica;
- Falha no sistema de resfriamento de equipamentos;
- Falhas de hardware, que impedem a entrega do serviço;
- Falhas de software, que impedem a entrega do serviço.

A prática para gestão de incidentes, segundo o framework ITIL 4 "Incident Management ITIL 4 Practice Guide" define três práticas essenciais para o sucesso da gestão de incidentes AXELOS (2020):

- Rápida identificação de incidentes;
- Resolução rápida e eficiente de incidentes;
- Evolução contínua do da gestão de incidentes

A rápida identificação de incidentes, permitirá que a recuperação do serviço também seja mais rápida, uma vez que seu tratamento será iniciado mais rapidamente. "Quanto maior a qualidade de dados iniciais, melhor será a resposta correta e a resolução de incidentes, incluindo resoluções automáticas." (AXELOS, 2020). O NOC foi criado justamente para esta prática, através das alarmísticas enviadas instantaneamente quando há alguma alteração no estado da rede (Monitoring and event management), para que o serviço seja rapidamente recuperado, e assim, categorizando a "Resolução rápida e eficiente de incidentes". Como a AXELOS define,

para simples incidentes reincidentes, a automação de tratamento/resolução é aconselhado, para diminuir o tempo de resolução e aumentar a eficiência. O modelo proposto por este trabalho passa justamente por esquematizar o processo de tratamento de incidentes simples e recorrentes, através da automação do reconhecimento de incidentes nas alarmísticas e posteriormente, automação da resolução.

Além disso, a prática para gestão de incidentes define dois processos, através das atividades do "Incident Management", sendo estas AXELOS (2020):

- Tratamento de incidentes e resolução: caracterizado em todo o fluxo de identificação de incidente até a sua resolução.
- Revisão periódica dos incidentes: processo que permite o aprendizado por meio dos incidentes, para que futuras abordagens sejam mais eficientes.

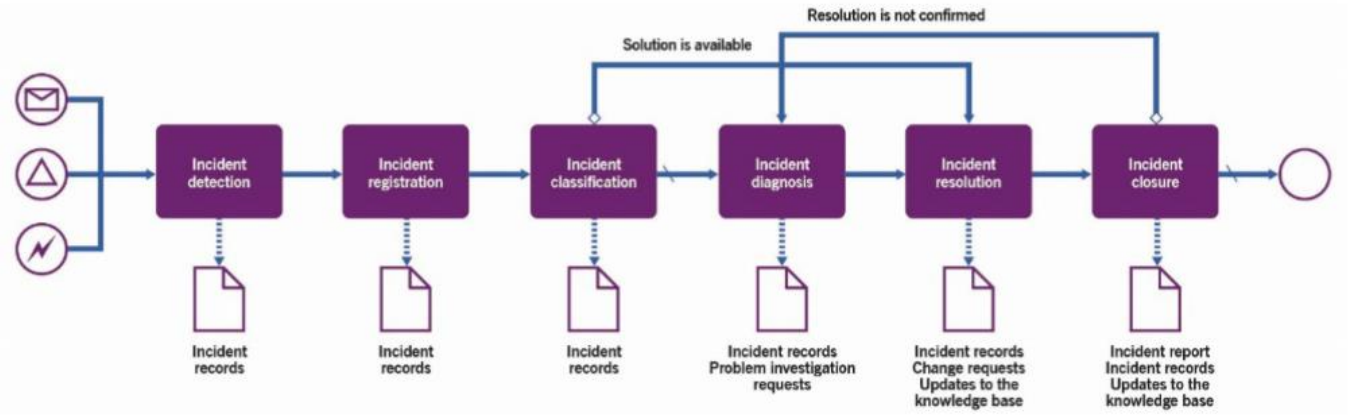


Figura 4: *Workflow do tratamento de um incidente e seu processo de resolução - retirado de: Incident Management ITIL 4 Practice Guide. AXELOS GLOBAL BEST PRACTICE. (2020)*

A gestão de incidentes de rede, é uma das principais funções do operador do Network Operation Center, como é definido pela figura 4. Através das alarmísticas que lhe são apresentadas, é detetado um evento na rede, que pode ser mapeado para um incidente (Incident Detection). Identificada a existência do incidente, é realizado o seu registo, bem como a sua verificação de reincidência, possíveis causas Incident Registration). Seguidamente, necessário classificar o tipo de incidente, o serviço associado, e a sua criticidade conforme as condições do nível de serviço acordado (Incident Classification). Após a classificação do incidente, é realizado um diagnóstico do mesmo, de forma a auxiliar na sua resolução (Incident Diagnosis e Incident Resolution). Com a resolução do incidente seguindo os respetivos procedimentos de

resolução, realiza-se uma confirmação de que o serviço foi recuperado, bem como os custos da resolução, uma investigação e revisão do incidente em questão, para assim, finalizá-lo. A disposição da alarmística de forma espontânea, ou seja, não intencionada, representa a alteração do equipamento de rede, e inicialmente é tratado como incidente. Uma vez que o modelo proposto atua no aparecimento da alarmística, em pleno funcionamento, garante que todos os alarmes sejam tratados como incidente durante o seu início. Durante a sua resolução, será efetivamente identificado se era uma falha de configuração, alarme falso, que ainda sim, é um incidente, mas que não foi identificado inicialmente. Sendo assim, o modelo proposto garante a atuação em toda alarmística apresentada, e consequentemente, todos os incidentes.

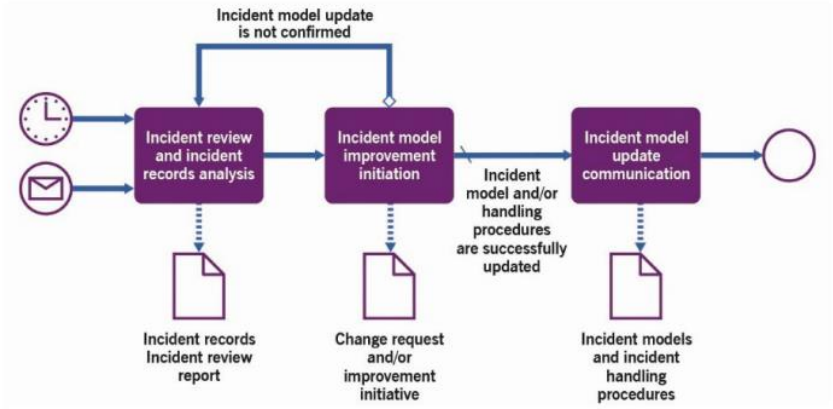


Figura 5: *Workflow da revisão periódica de incidentes – retirado de: Incident Management ITIL 4 Practice Guide. AXELOS GLOBAL BEST PRACTICE. (2020)*

O outro processo relativo à gestão de incidentes definido no ITIL 4, é a revisão periódica dos incidentes. Apesar de não ser responsabilidade do NOC, trata-se um processo imperativo para evolução das práticas de gestão de incidentes. Através da revisão dos incidentes, é possível identificar padrões e diagnósticos que poderão auxiliar em incidentes futuros, estabelecendo procedimentos de resolução, garantindo uma maior eficiência na resolução das avarias, ou até mesmo, identificando situações em que a entrega do serviço não esteja em plenas condições, e assim haja maior eficácia. A Figura 5 caracteriza o fluxo desse processo, subdivido em três atividades principais: A primeira atividade diz respeito à revisão de incidentes e análise do registo de incidentes – o gestor de incidentes, aliado com o responsável do serviço e partes interessadas relevantes, selecionam incidentes específicos para proceder à sua análise focando a eficiência e eficácia com que estes foram resolvidos-. Eles identificam oportunidades para um

modelo mais eficaz para gestão de incidentes ou otimização de processos. Numa atividade posterior, procuram melhorar o modelo de gestão de incidentes. O Gestor de incidentes, regista as iniciativas de melhorias para serem implementadas em conjunto com a evolução contínua de incidentes ou inicia diretamente um pedido de alteração (RFC). – Por fim, a última atividade corresponde à comunicação da atualização do modelo de gestão de incidentes. Se o modelo de gestão de incidentes foi devidamente atualizado, é realizado a comunicação para as partes interessadas relevantes. Normalmente é realizada pelo gestor de incidentes e/ou pelo responsável pelo serviço ou pelo proprietário do recurso. A revisão periódica dos incidentes é uma ação para auxiliar na estruturação das melhores práticas de resolução de cada incidente, para aumentar a eficiência (AXELOS, 2020)

A gestão de incidentes atua principalmente no âmbito de uma ação reativa, ou seja, age em resposta aos incidentes que lhe são apresentados. Conforme indicado anteriormente, a revisão dos incidentes, permite a identificação de situações que necessitam alteração da entrega do serviço proposto. Em uma situação hipotética em que uma antena que realiza a entrega de serviços de dados móveis que, constantemente está a ter quebras de serviço por problemas de energia, através da revisão de incidentes, é possível identificar a situação, e garantir com que o problema seja resolvido de forma definitiva, como por exemplo, realizado um aumento da capacidade elétrica do local. Este tipo de alterações é garantido através da "Gestão de Alterações". Nesta prática, definida pelo ITIL 4 como "Change Enablement", uma alteração é definida como: "a adição, modificação ou remoção de qualquer coisa que possa afetar os serviços de TI.", ou seja, toda e qualquer alteração, que tenha algum impacto no serviço, como mudanças na infraestrutura, mudanças processuais, de fornecedores, ou outro qualquer componente que suporte o serviço. ITIL ainda determina três tipos diferentes de alterações:

- Alterações Standard: Alterações pré-autorizadas, com baixo risco no serviço.
- Alterações de Emergência: Mudanças que devem ser implementadas imediatamente.
- Alterações Normais: Mudanças planeadas que muitas vezes são implementadas no âmbito de projetos.

O NOC encontra também no seu dia-a-dia, algumas atividades relativas a gestão de pedidos. Definido pela BMC Software, em "Service Request Management in ITIL 4", um pedido é uma solicitação de um utilizador ou representante autorizado de um utilizador, que inicia uma ação

de serviço que foi acordada como parte normal da prestação de serviço. Ou seja, tem como propósito, valorizar e melhorar a qualidade de serviço, mediante as solicitações de algum utilizador do serviço. Toda a parte de gestão de pedidos depende de processos estruturados, suportados por ferramentas próprias. Para o operador do NOC, essas solicitações não são utilizadas como respostas a alguma falha ou degradação do serviço, uma vez que estes são incidentes. Contudo, podem estar cientes de algumas requisições de serviço que cause algum impacto para a rede.

As responsabilidades do técnico do Network Operation Center concentra-nestas três grandes atividades:

1. Gestão de Incidentes
2. Gestão de Alterações
3. Gestão de Pedidos

Todos os processos definidos pelo ITIL, e geridos pelo ITSM são de extrema importância para que o serviço disponibilizado seja entregue da melhor forma possível. Portanto, é de suma importância que todos os processos sejam bem estabelecidos, para que sejam bem monitorados, e assim, aumente a resiliência dentro da organização.

2.2.1 Equipas parceiras

Um processo vital para o funcionamento de um Network Operations Center, é o estabelecimento de equipas parceiras, seja de terreno, seja de suporte de operações, para que os incidentes que tenham o menor tipo de impacto no serviço para os clientes. Para isso, a organização que garante um serviço IT, determina o estabelecimento de um SLA (Service Level-Agreement) entre ambas as partes. O SLA é definido pelo ITIL 4 como um acordo entre um provedor de serviços IT e um cliente, no qual são definidas regras, responsabilidades e metas das duas partes, por exemplo, o cumprimento do Recovery Time Objective (RTO), ou seja, o tempo aceitável para a recuperação dos serviços, após um incidente/desastre.

O Network Operations Center é a área que interliga o IT Service Provider com a organização com a qual foi estabelecida o SLA. Como determinado no tópico 3.1, uma das suas funções de uma operador NOC é o diagnóstico e o remediar do incidente anteriormente identificado. Caso a resolução ultrapasse as capacidades do técnico, aciona-se a organização definida no SLA,

uma equipa parceira, para que possa solucionar a avaria identificada, dentro do RTO estabelecido. É de função do NOC monitorar o cumprimento das metas estabelecidas pelo SLA, para que não haja um grande impacto para os utilizadores do serviço disponibilizado.

2.3 Automatismos de Processos

Toda a supervisão realizada pelo Network Operation Center ocorre por meio de alarmes que são enviados pelos equipamentos que compõem a rede. Cabe ao operador definir quais são os eventos da rede, e quais são os incidentes, através da gama dos alarmes que lhes são disponibilizados. Toda alarmística apresentada decorre-se por meio de um protocolo de rede vital para a permissão de monitoramento e gestão de rede: SNMP – Simple Network Management Protocol.

O SNMP é definido como "um protocolo na camada de aplicação para transmitir controlo de gestão de rede e mensagens de informação entre um servidor e um agente executando em nome desse servidor de gerenciamento." (Kurose & Ross, 2017, p. 423). Todo equipamento estabelecido na rede tem na sua configuração, protocolos SNMP que comunicam com o servidor o estado de funcionamento. O SNMP é o sucessor do SGMP (Simple Gateway Management Protocol) definido para a gestão de routers, contudo "o SNMP pode ser utilizado em sistemas Windows, impressoras, modem racks, fontes de alimentação de energia, entre outros." (Mauro & Schmidt, 2001, p. 7). Todo software ou hardware pode recolher informação por meio do SNMP, o que aumenta a gama de informação concebida ao nível de alarmística.

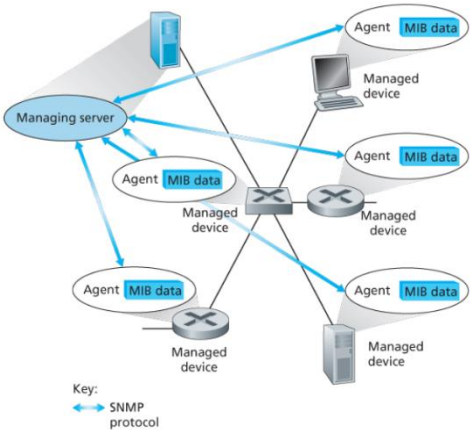


Figura 6: *Elementos de uma Gestão de Rede. - retirado de: "Computer Network - A Top-Down Approach (7th edition)." (Kurose & Ross, 2017, p. 422)*

A Figura 6 demostra os elementos e o funcionamento de uma rede com gestão por meio do SNMP. Cada equipamento supervisionado, tem a sua comunicação com o servidor de gestão por meio do protocolo SNMP, este equipamento, como apresentado anteriormente, pode ser um router, switch, modem, baterias, servidores, desde que esteja presente dentro da rede que está em monitoramento. As informações de cada equipamento são recolhidas e agregadas por meio do MIB (Management Information Base), definidas pelo "Managing Server".

Por fim, o "Managing Server" é definido como "uma aplicação, tipicamente com um humano no 'loop', integrados em uma Estação de Gestão de Rede Centralizada no Network Operations Center. O Managing Server é o locus de atividade para a gestão de rede; controla a recolha, processamento, análise e/ou a apresentação de Informação para a Gestão de Rede." (Kurose & Ross, 2017, p.423). Neste ponto que as alarmísticas são apresentadas e dispostas para a análise do operador do NOC.

Cada alarmística apresentada, como referido no início, será distinguida de evento ou incidente, e caso seja um incidente, terá o registo e início de resolução. Os automatismos processuais iniciam-se nesta etapa, quando há a disponibilização dos alarmes, pois cada alarmística ou o conjunto delas, tem o seu grau de importância e relevância dentro de um incidente de rede. Por exemplo, um corte de uma fibra ótica, não tem o mesmo grau de importância ou complexidade de resolução, do que uma falha de uma bateria em uma estação móvel, uma vez que uma tem impacto direto quanto ao serviço do cliente, e a outra não dispõe de nenhum impacto para o utilizador.

A dificuldade deste processo de automatismo, é compreender e estabelecer uma relação de cada alarmística que é apresentada, seja individualmente, ou num conjunto. Este automatismo tem a tarefa facilitada com Machine Learning, onde por meio de ação, tentativa e histórico, é possível aprender e desenvolver o conhecimento sobre os processos realizados por cada situação (Mohammed, A. & Côte, 2021).

2.4 Ferramentas de Suporte

Conforme apresentado no 2.3, o Managing Server é a aplicação agregadora de alarmes, e por meio de "views", permite o monitoramento da rede. Contudo, o fornecedor, quando dispõe dos seus equipamentos para a montagem da rede, também dispõe de um software próprio, que não

só detém a alarmística, mas também das configurações, permitem o acesso para resoluções da 1ª/2ª linha, através de restarts, verificação do estado do equipamento, entre outras. A alarmística de cada software, conectam-se ao Managing Server, e assim permitir a agregação de todos os alarmes. Fornecedores como TEOCO, Solarwinds, ManageEngine, disponibilizam de "Fault Management Software" que realizam a função de um Managing Server, permitindo a integração da alarmística do equipamento de outros fornecedores em uma única plataforma.

Outra plataforma intrínseca para a aplicação do automatismo, é um software que disponibiliza o serviço do ITSM, como, por exemplo, a BMC Remedy IT Service, Jira Service Management. Juntamente com o Managing Server, por meio de uma API, faz-se a interligação entre essas duas plataformas, para a criação dos tickets dos incidentes da rede, e iniciar o processo de atuação do NOC.

Na documentação da BMC Remedy IT Service, há a sugestão da utilização de REST API para automatização de processos. Uma API (Application Program Interface) é definida como uma série de regras que definem a comunicação e conexão entre aplicações ou equipamentos, uma REST API (ou RESTful API) é uma API que tem o seu design a partir do REST (Representional State Transfer). Os princípios de uma arquitetura REST foram definidos por Roy Thomas Fielding, 2000, em "Architectural Styles and the Design of Network-based Software Architectures", caracterizado pela seguinte estrutura:

- Client-server: O estabelecimento de duas forças bem definidas: cliente e servidor. Ao separar a UI (User Interface) das preocupações de armazenamento de dados, permite uma melhoria da portabilidade da interface em múltiplas plataformas, juntamente com a melhoria da escalabilidade, ao simplificar os componentes do servidor, ou seja, cada componente tem um desenvolvimento independente.
- Stateless (sem estado): O cliente não pode se aproveitar dos recursos do servidor, ou seja, toda a solicitação do cliente para o servidor deve conter todas as informações necessárias para que a solicitação seja cumprida, o estado da sessão e do andamento da comunicação é todo armazenado no lado do cliente.
- Cache: cache é um dispositivo interno a um sistema, utilizado como um intermediário entre um processo e o armazenamento, para acesso rápido por parte do operador. Para tornar a comunicação mais eficiente, cada dado é definido como "cacheable" ou "non-

cacheable". Caso seja "cacheable", o cache do cliente poderá reutilizar aquela informação para futuras solicitações, e assim, capacitar mais eficiência, performance e escalabilidade de processos.

- Interface uniforme: "O recurso central que distingue a arquitetura REST de outros estilos baseados em rede é a sua ênfase em uma interface uniforme entre todos os componentes. Ao aplicar o princípio de generalidade da engenharia de software à interface do componente, a arquitetura geral do sistema é simplificada e a visibilidade das interações é aprimorada." (R. Fielding, 2000) A uniformidade da interface por meio do REST é desenhada para ter eficiência perante "hypermedia data transfer", uma das principais transferências utilizadas na Web.
- Sistema por camadas: Uma arquitetura por camadas permite a criação de hierarquias e independência para os diversos componentes do sistema, além da redução da complexidade da solução.
- Code-on-demand: Uma das principais funcionalidades para a proposta de solução apresentada é esta característica. O "code-on-demand" permite com que recursos sejam adicionados após a implementação, como uma extensão do sistema.

Essas são as principais características que constituem a arquitetura de uma RESTful API. A comunicação por meio desta arquitetura é estabelecida por meio de solicitações por HTTP, para a execução de ações pré-definidas como "GET", "POST", "PUT" e "DELETE", que são entregues por meio de diversos formatos como HTML, JSON, Python ou texto simples. Por exemplo, através do Postman, uma plataforma de teste e desenvolvimento de APIs, é possível interligar os processos de ITSM e o Managing Server.

Com estabelecimento desta API entre essas duas plataformas, pode-se iniciar os processos de automatismos. Criando um modelo de incidentes, conforme o guia de boas práticas de gestão de incidentes pela AXELOS, permite a eficiência da sua resolução. Através das ferramentas de suporte citadas, o operador NOC terá maior eficiência no seu curso de trabalho, e consequentemente, uma maior estabilidade da rede.

3 Metodologia

Para estruturar e organizar o decorrer do planeamento, o projeto terá a metodologia de "Design Science Research". O DSR (Design Science Research) é um paradigma "que busca desenvolver conhecimentos humanos com a criação de artefactos inovados e com a geração de 'design knowledge' (DK) por meio de soluções inovativas para problemas do mundo" (Hevner, et al, 2004). Ou seja, o DSR busca, por meio da definição de ações, conquistar um objetivo final, de forma organizada e estruturada.

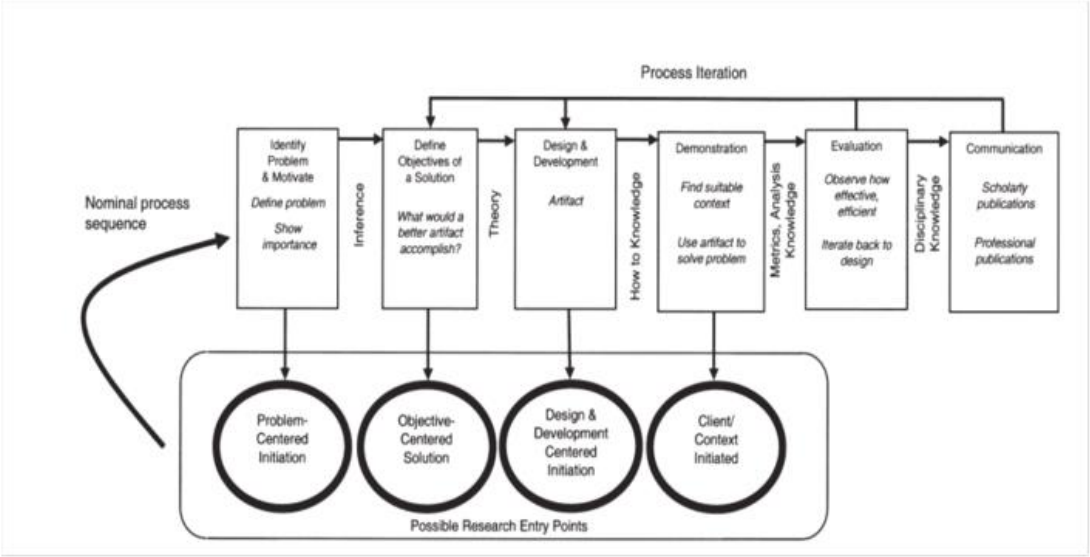


Figura 7: *Modelo processual da metodologia Design Science Research (vom Brocke, Hevner, Maedche, 2020)*

Um exemplo de um modelo processual do Design Science Research está definido na Figura 7, na qual estão definidos seis tópicos:

- Identificação do problema e motivo (Diagnóstico): Por meio de análises, resultados, busca definir um problema. Hevner & vom Brocke (2020) explicaram a importância deste passo, pois através dele motiva o investigador e a sua "audiência" para buscar a sua solução, e também permite com que sua "audiência" compreenda o motivo da busca por solucionar.
- Definir objetivos para a solução: processos necessários e importantes para a conquista da solução. A cadeia de objetivos deve cumprir os requisitos SMART (Specific, Measurable, Achievable, Relevant e Time-bound), para que facilite o seu controlo e a sua importância dentro de todos os objetivos definidos.

- Design e desenvolvimento: neste tópico é definido o modelo de solução, para determinar o seu valor, os recursos necessários para a sua execução, bem como o funcionamento ideal, para servir de parâmetro futuramente.
- Demonstração: por meio de uma parte do problema, definir a sua eficácia. Hevner & vom Brocke (2020) exemplificam formas de mensurar a demonstração com experimentos, simulações, *case study* ou outra atividade que seja relevante para a apresentação de resultados.
- Definição de resultados: com os resultados da demonstração, há "definição de resultados". Como referido anteriormente, este tópico busca mensurar a eficácia do modelo proposto, por meio da comparação dos objetivos, com os resultados observados.
- Comunicação: "Comunicar o problema e sua importância, o modelo, sua utilidade e novidade, o rigor do design, e sua efetividade para os investigadores e para o público-alvo" (Peffers et al, 2006). Ou seja, é transmitir os resultados observados pelo modelo a quem será aplicado, como profissionais exercem funções que estão definidas no modelo, como por exemplo, em uma alteração de sistema operativo, seria a comunicação para todos os profissionais que estão sujeitos à mudança, mas também aos stakeholds, por exemplo.

4 Design da Solução

4.1 Análise da Situação Atual (AS-IS)

O modelo proposto qualifica a implementação para um NOC que não consiste de nenhum automatismo presente, e somente os seus requisitos básicos (Managing Server, Plataforma de ITSM e Softwares dos fornecedores). Conforme citado por A.Mohammed, et al (2021), grande parte dos processos para tratamento de falhas são realizadas manualmente ou possuem regras estruturadas por experts. Ou seja, a proposta de solução baseia-se no automatismo de avarias de rede que são reincidentes, com pouco impacto, para direcionar o foco do operador NOC em avarias de rede com maior impacto, para assim, maximizar o QoS.

Atualmente, o NOC analisado possui todo o processo de registo e tratamento de incidentes de forma manual, o que aumenta a duração da resolução do incidente e além disso, permite falhas, conforme citado anteriormente. A proposta de solução busca automatizar todo o processo de identificação, registo, diagnóstico e resolução do incidente, sem atuação do operador do NOC.

Portanto, para auxiliar e estruturar o automatismo, é imperioso a implementação de uma equipa de desenvolvedores, para iniciar a estruturação dos processos. Esta equipa estará encarregada de realizar a interligação de alarmística básica com a plataforma de ITSM, sem intervenção do operador do NOC, com tratamento completamente automatizado. A interligação entre o Managing Server e o ITSM será realizada por meio do Postman RESTful API, que permite, por meio de *requests*, buscar informações dos tickets na plataforma de ITSM (BMC Remedy), a partir do estado do alarme no Managing Server (TEOCO Fault Management).

Atualmente, um operador NOC pratica diversas atividades simultaneamente, além da validação dos incidentes de rede, Miloslavskaya (2018) descreveu as seguintes atividades de um técnico do Network Operations Center:

- Suporte contínuo para alta disponibilidade da rede;
- Desempenho (como falha de energia, alarmes de falhas de comunicação, erros de bit, circuitos inativos, entre outras situações que podem afetar a rede), monitoramento, relatórios, melhorias, recomendações e rastreamento de problemas até que sejam resolvidos.

- Constante pesquisa de anomalias e resoluções de alarmes críticos, isolar os problemas, identificar as causas, criação de tickets, ajustar as avarias de redes e escalar as questões de urgência.
- Gerir: domínios, configurações, armazenamento, emails, tráfego voz e vídeo, suporte aos usuários finais.
- Otimização da qualidade de serviço e reporte das situações de degradação de serviço.
- Cumprimento dos acordos de níveis de serviço (SLA).
- Coordenação com redes afiliadas;
- Controlos básicas de IS como autenticação e autorização, filtragem de endereços IP e MAC.

Conforme citado pela AXELOS, em "Incident Management ITIL 4 Practice Guide", são definidas três práticas essenciais para o sucesso do Incident Management: Identificação rápida de incidentes; resolução rápida e eficiente de incidentes; e por fim, evolução contínua do "Incident Management". Tendo em vista a vasta quantidade de atividades de um operador do NOC, a solução propõe a tratar incidentes de menor impacto, conforme descrito anteriormente, de forma automática, para maior rapidez e eficiência, para assim, diminuir a carga de atividades do operador NOC, e evoluir a capacidade do operador de gerir incidentes de maior impacto (Incident Management).

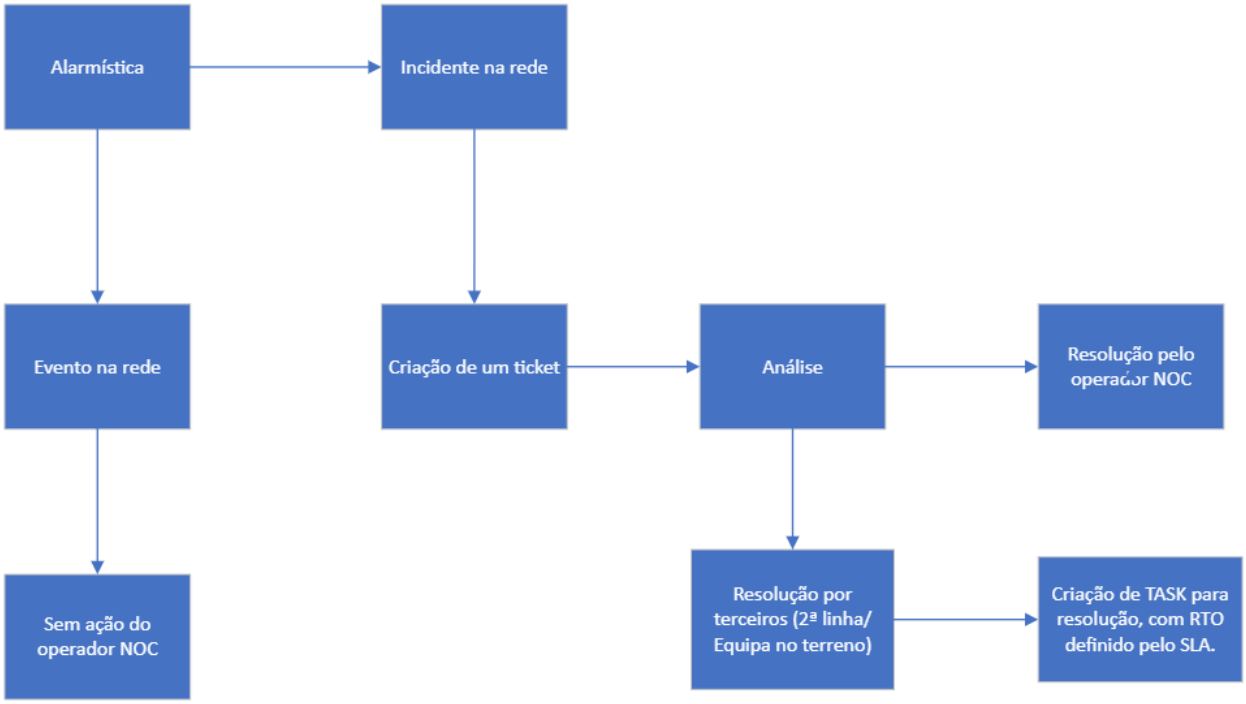


***Figura 8**: Workflow atual de funcionamento do NOC. - Realizado pelo autor.*

A Figura 8 caracteriza o método de trabalho de um operador NOC, em busca de solucionar um incidente de rede, por meio das alarmísticas apresentadas. Como citado anteriormente, os tratamentos de incidente de rede, desde o seu registo, até a sua análise, são efetuados manualmente pelo operador NOC. Inicialmente, são dispostas as alarmísticas da rede, e por regras estabelecidas por experts, ou até mesmo pelos fornecedores dos equipamentos, são definidos os eventos que também são caracterizados como incidentes. Um evento é definido pela ITIL como qualquer ocorrência detetável que possui importância para a gestão dos serviços de TI, são basicamente notificações da ferramenta de monitoramento. Ou seja, um sistema que está mais lento que o usual, caracteriza um evento que não é incidente, contudo, a partir do momento que este sistema iniciar a sua afetação no serviço, trata-se de um evento-incidente.

Após a distinção de evento-incidente, há o registo da situação por meio da criação de um ticket. Nesta etapa, concentra-se a qualificação de ITSM, e todo o âmbito de "Incident Management", no qual o operador registar-lhe-á toda e qualquer relevante informação para o incidente em questão, de forma a não só auxiliar a resolução da avaria, mas também para análises futuras. No âmbito da análise, o operador NOC realiza todo o diagnóstico possível, e

caso esteja no âmbito do NOC, tentar solucionar, caso esteja fora de atuação, reporta-se para qual equipa for necessária (2ª linha ou equipa de terreno).

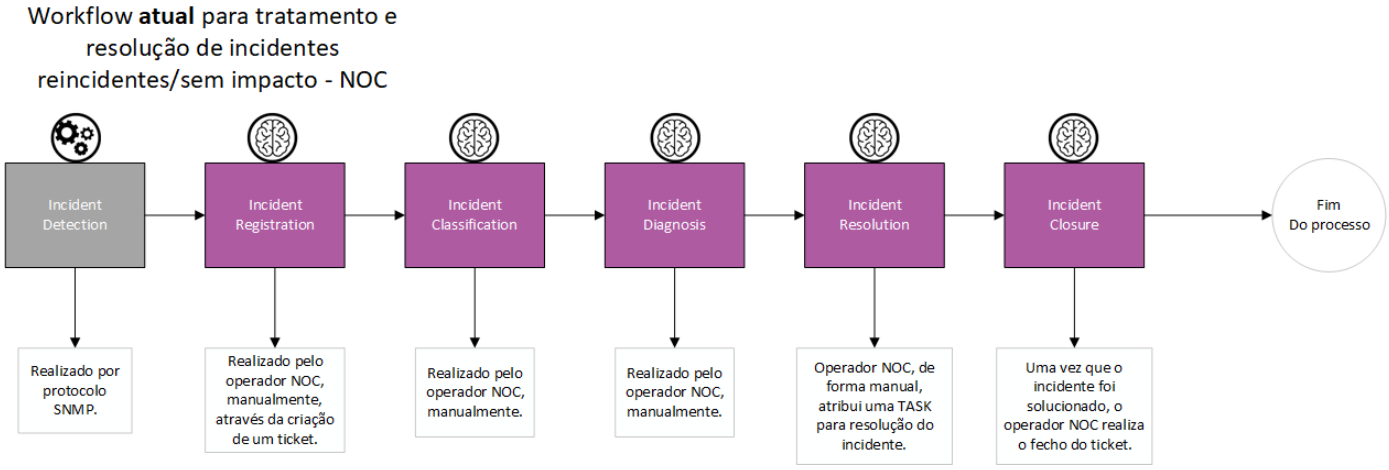


Figura 9: *Workflow atual para tratamento de incidentes reincidentes e sem impacto no NOC. - Realizado pelo autor.*

A Figura 9 exemplifica o processo atual para resolução de incidentes reincidentes e sem impacto. A criação do incidente é realizada diretamente no Managing Server, uma vez que o operador verifica que o alarme está ativo, cria um ticket e realiza os restantes processos manualmente, como a classificação, diagnóstico (uma vez que são reincidentes e sem impacto para a rede, o diagnóstico é reincidente) e endereçam para a sua resolução. Uma vez que o incidente está solucionado, o operador NOC, manualmente, valida se a alarmística está ativa, e uma vez que o incidente está resolvido, finaliza o ticket na plataforma de ITSM.

4.1.1 Especificação de requisitos

Durante a fase de Especificação de requisitos, são definidas as funções e a performance do software, para direcionar a sua utilidade. Estão divididos em funcionais, que apresentam as funcionalidades da proposta, e os não-funcionais, que demonstram os detalhes a nível técnico.

4.1.1.1 Requisitos funcionais

- Criação/Fecho do registo de incidente (ticket) em plataforma de ITSM.
- Criação/Fecho de tarefa para resolução de incidente em plataforma de ITSM.
- Validação do estado da alarmística.

4.1.1.2 Requisitos não funcionais

- Managing Server (plataforma agregadora de alarmes – TEOCO Fault Management Software).
- Plataforma de ITSM (BMC Remedy).
- APIs para ligação entre o Managing Server e ITSM (Postman API).
- Segurança e disponibilidade.
- Performance e produtividade.
- Eficiência.

4.1.2 Casos de uso

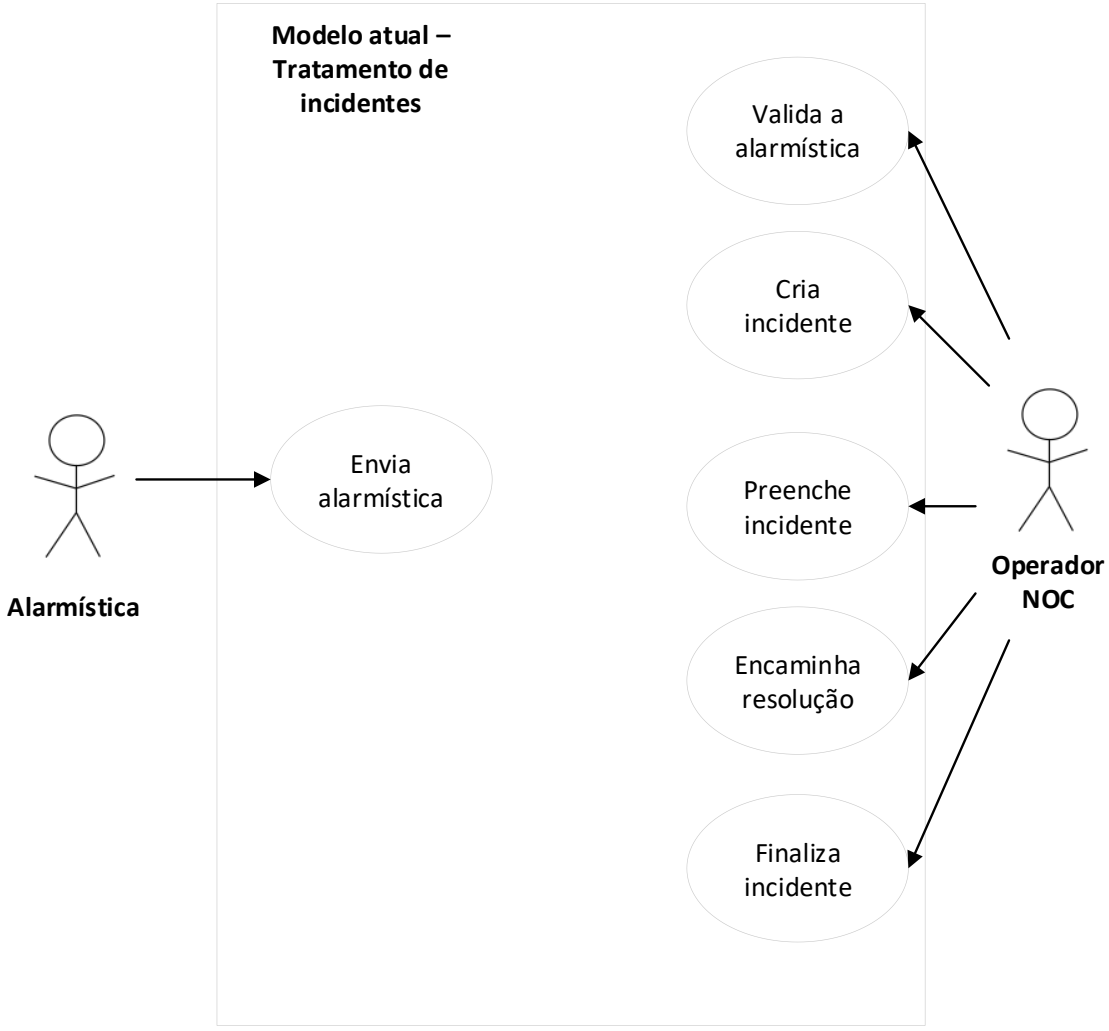


Figura 10: *Caso de uso, modelo atual de tratamento de incidentes no NOC. - Realizado pelo autor.*

A Figura 10 ilustra o modelo atual de tratamento de incidentes no NOC, com dois atores principais: alarmística – enviado pelos equipamentos de rede, armazenada no Managing Server -, e o Operador NOC. A única função da alarmística é efetivamente dispor os alarmes para que o operador possa atuar. O agente do NOC é responsável por toda criação, registo e finalização do incidente, perante a validação da alarmística, ou seja, se o alarme está ativo, o NOC atua, realiza o registo e encaminha à sua resolução, uma vez que o alarme já não está ativo, o NOC finaliza o incidente, pois o equipamento retornou ao seu estado de origem.

4.2 Desenho da solução: Modelo Operativo para NOC

Conforme descrito no Capítulo 2, na Figura 4, pela AXELOS (2020) em "Incident Management ITIL 4 Practice Guide", o tratamento de um incidente ocorre por seis passos: Identificação do incidente; registo de incidente; classificação do incidente (impacto); diagnóstico do incidente; resolução do incidente; fecho do incidente. A solução explora todos os passos apresentados, com exceção do diagnóstico, que por sua vez, não terá muita importância, pois são incidentes sem maior impacto na rede.

A Figura 11 aliada à tabela 1, demonstra o *workflow* da proposta de solução, que através do monitoramento do estado do alarme, irá validar se o incidente existe ou não. Caso o alarme esteja ativo, será iniciado o processo de criação do registo de incidente em Postman API. Caso o alarme não permaneça, será finalizado o ticket de registo de incidente

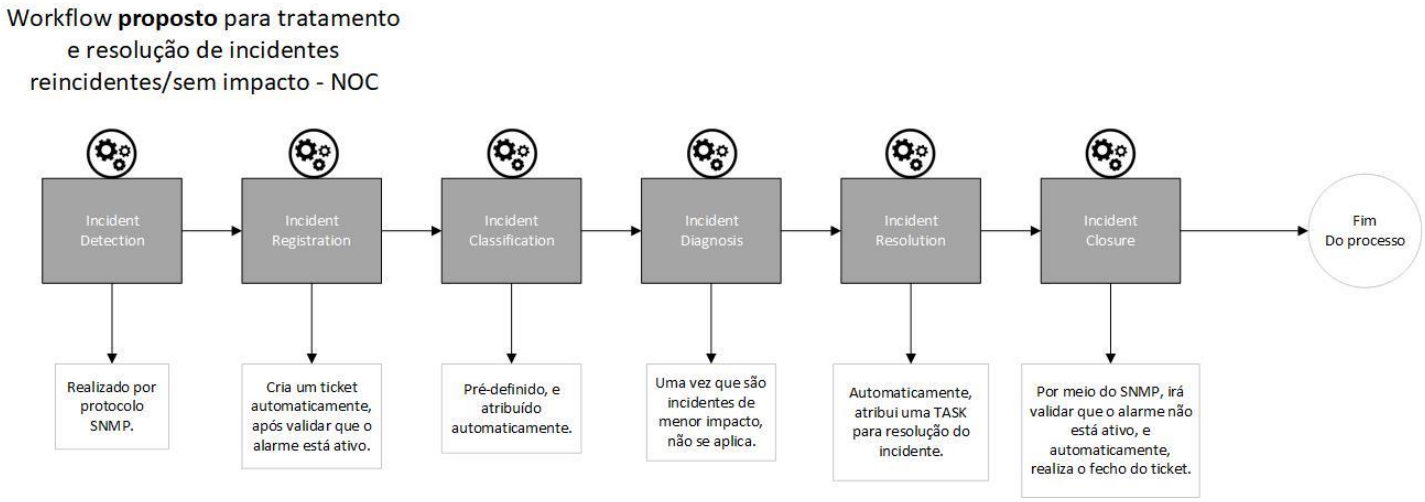


Figura 11: *Workflow proposto para tratamento e resolução de incidentes reincidentes e sem impacto no NOC. - Realizado pelo autor.*

Workflow para tratamento e resolução de incidentes – AXELOS (2020)	**Atuação da solução apresentada**
Incident Detection	Verifica constantemente se o alarme está ativo, por meio de protocolos SNMP.
Incident Registration	Uma vez que o alarme está ativo, realiza o registo de incidente (ticket) na plataforma ITSM.
Incident Classification	A classificação do incidente é pré-definida, através da classificação enviada pelo NOC. Cada alarme possui uma definição (Minor, Major e Critical), a solução atual propõe o tratamento da alarmística "Minor", propondo a evolução para tratamento dos restantes tipos no "Trabalhos Futuros".
Incident Diagnosis	Não se aplica, pois, a solução implica o tratamento de alarmísticas simples, sem impacto para o utilizador final.
Incident Resolution	Será encaminhado para a verificação e resolução do parceiro de terreno (TASK).
Incident Closure	Por meio dos protocolos SNMP, será validado o estado do alarme, e uma vez que não estiver mais ativo, o incidente terá sido solucionado, e, automaticamente, procederá para o fecho do ticket.

Tabela 1: *Tópicos para tratamento e resolução de incidentes presentes na solução. - Realizado pelo autor.*

A proposta da solução, além de direcionar o foco do operador NOC para o tratamento de incidentes que impactam o usuário final da rede, permite catalogar, registar e solucionar, com maior eficiência, os incidentes reincidentes de rede com menor impacto/sem impacto, e assim, buscar alguma solução para diminuir a sua frequência.

4.2.1 Diagrama de Fluxos

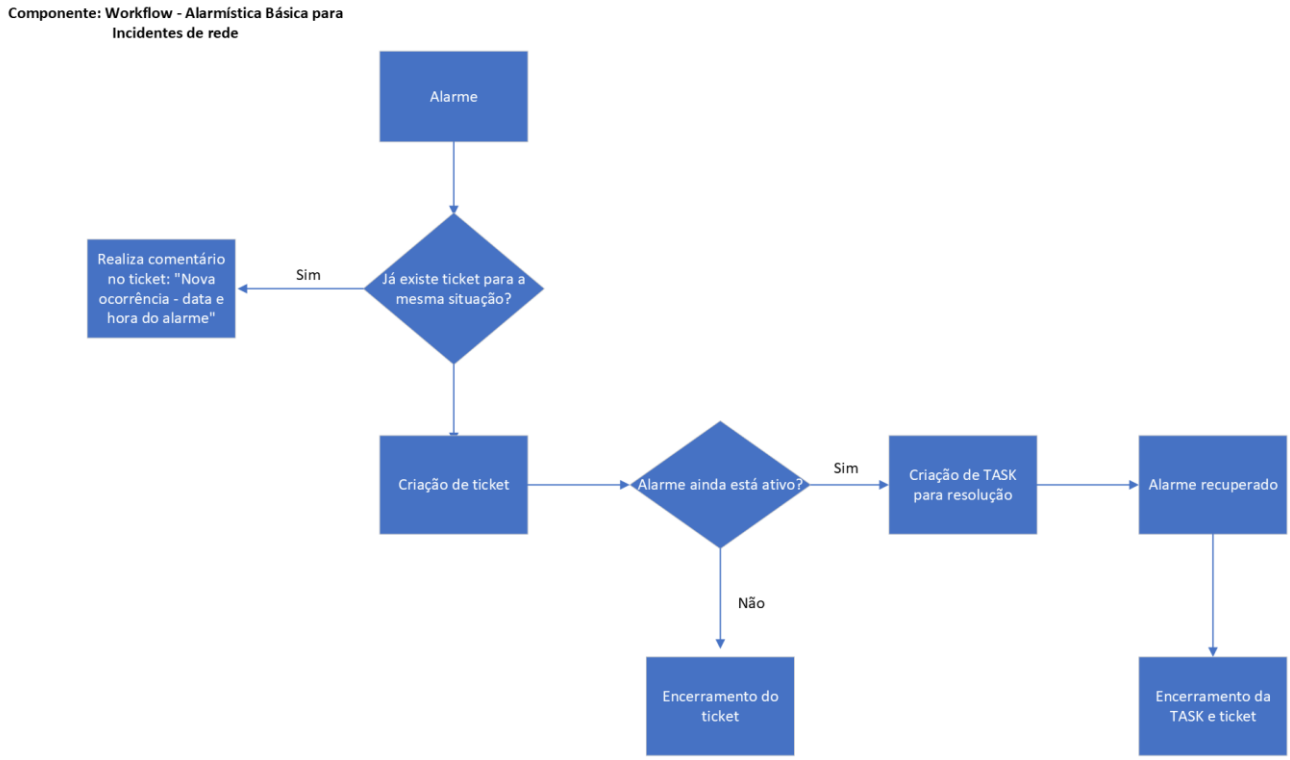


Figura 12: *Workflow de funcionamento da API proposta. - Realizado pelo autor.*

A Figura 12 demonstra o Workflow da solução para criação do tratamento e registo de incidentes básicos de rede, por meio das alarmísticas apresentadas. Quando a alarmística, que será pré-definida pelos desenvolvedores da aplicação, juntamente dos operadores NOC, for disposta no Managing Server, será verificada a existência de um ticket para a mesma situação, para não criar duplicatas para o mesmo incidente de rede, caso não existe, criar-se-á um ticket e registo de avaria. Posteriormente, será feita a validação do estado do alarme, caso esteja ativo, será encaminhado para a verificação pelo parceiro de terreno, para soluciona-lo. Uma vez que o alarme não estiver mais ativo, o ticket será fechado automaticamente.

Toda a validação é realizada pelo Postman RESTful API, por meio de *requests* do cliente (TEOCO Fault Managing – Managing Server) ao servidor (BMC Remedy), para buscar informação de tickets criados para a mesma situação, e posteriormente, criar ou terminar um registo de incidente.

4.2.2 Casos de Uso – Modelo Proposto

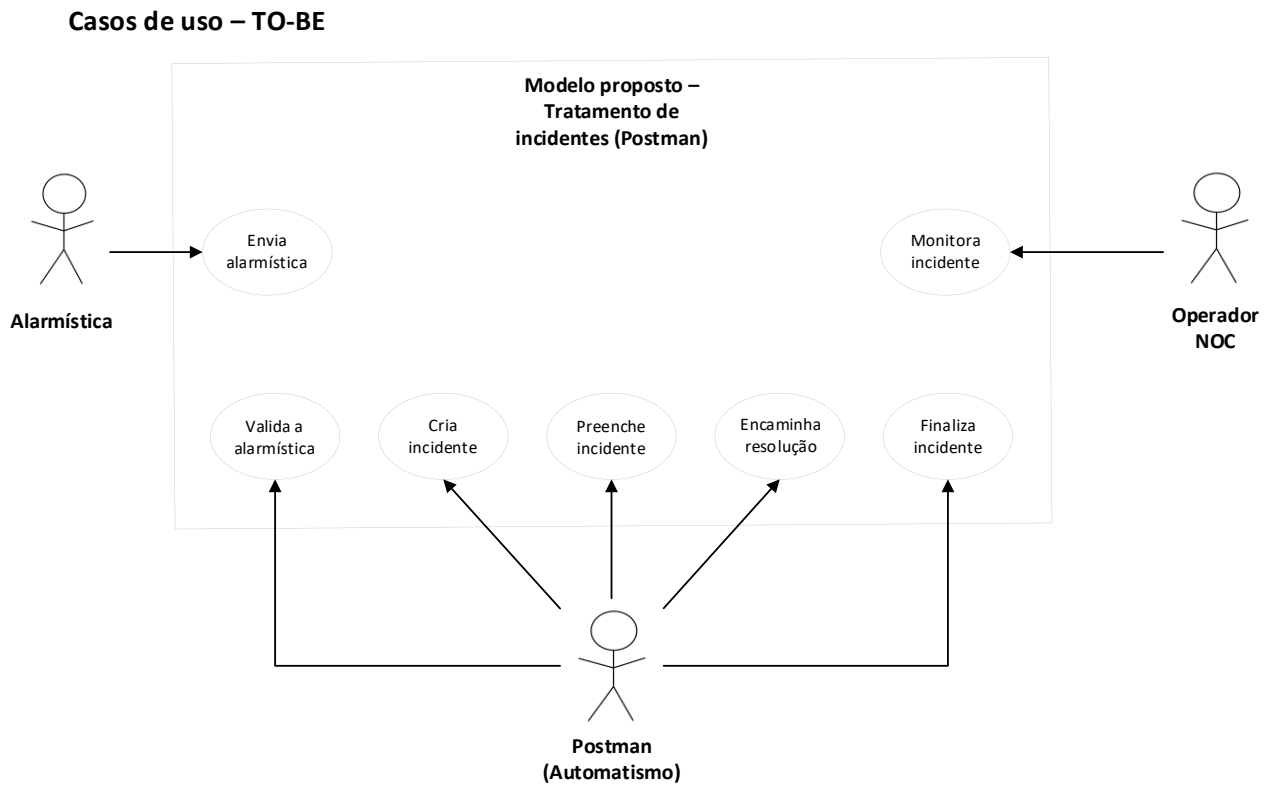


Figura 13: *Modelo proposto para tratamento de incidentes no NOC. - Realizado pelo autor.*

A Figura 13 apresenta os Casos de Uso para o modelo proposto, no qual o tratamento de incidentes será realizado de forma automatizada. Conforme verificado anteriormente, o modelo atual tem como o seu principal autor o "Operador NOC", responsável por toda a parte de catalogar e finalizar o incidente, contudo, o modelo proposto tem um novo autor: Postman API. O Postman será responsável pelas tarefas que antes era de cunho de atuação do NOC. O modelo inicia-se uma vez que o alarme está ativo, no qual o Postman tratará da criação do registo do incidente, e caso o alarme desapareça, finaliza o registo. O NOC terá como responsabilidade, no modelo proposto, realizar o monitoramento da criação, de maneira que consiga identificar possíveis falhas de tratamento, pelo menos em estado inicial.

4.2.3 Diagrama e Arquitetura do Sistema Operacional

O sistema operacional está estabelecido conforme ilustrado pela Figura 14. Através das três plataformas (TEOCO Fault Managing, BMC Remedy ITSM e Postman API) são definidos os processos anteriores, para a criação e registo de incidentes sem impacto. Caso o alarme esteja

ativo, irá decorrer o processo descrito na Figura 12, o Postman API irá realizar a validação se já há um ticket criado em BMC Remedy ITSM para o incidente, por meio de um *request* (GET), e caso não esteja, irá solicitar um outro *request* (POST), desta vez para criar e preencher o registo de incidente. Uma vez que o alarme não esteja ativo, a API realiza um novo *request* (PUT), de forma a finalizar o ticket em ITSM.

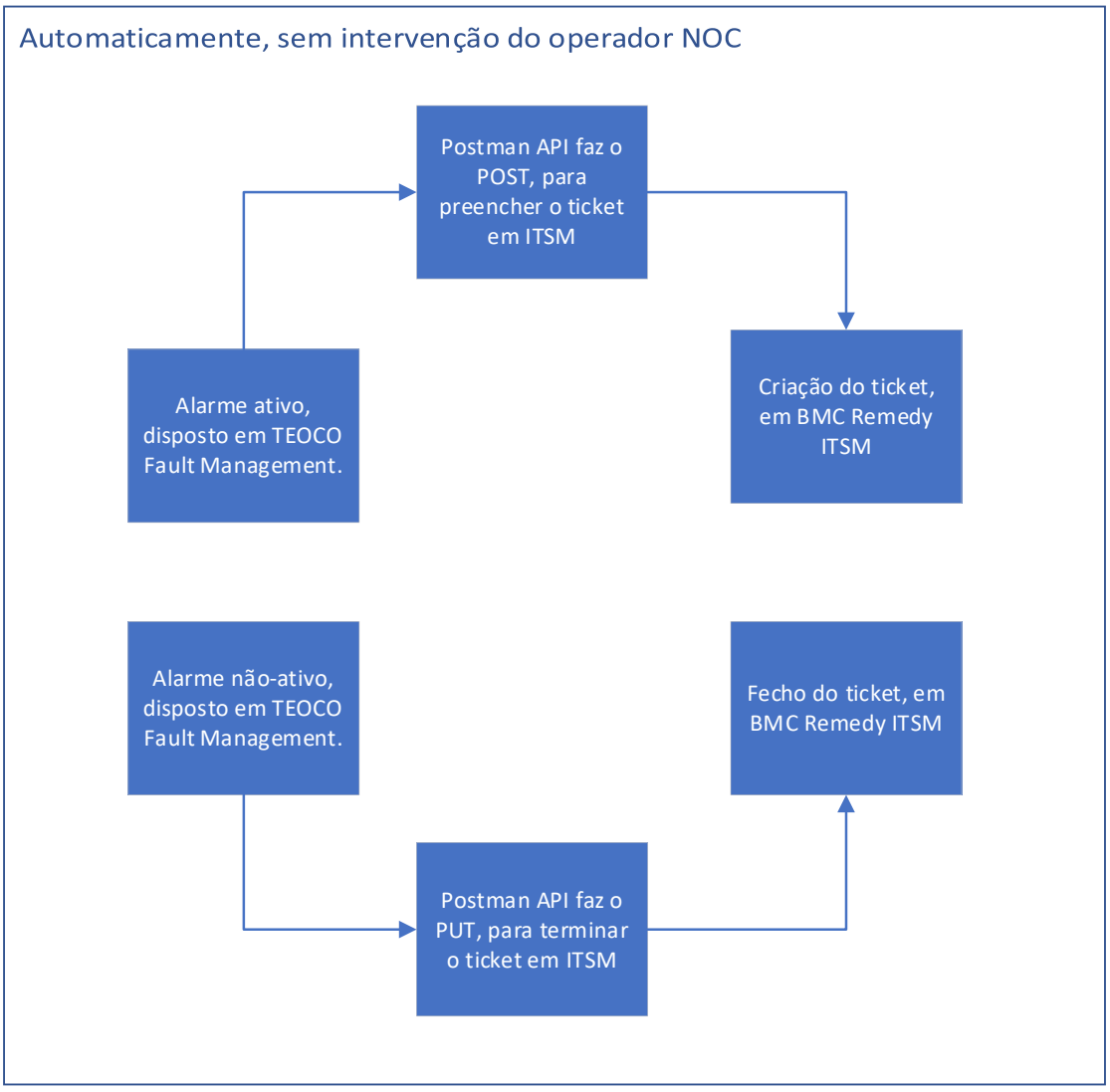


Figura 14: *Diagrama do Sistema Operacional. - Realizado pelo autor.*

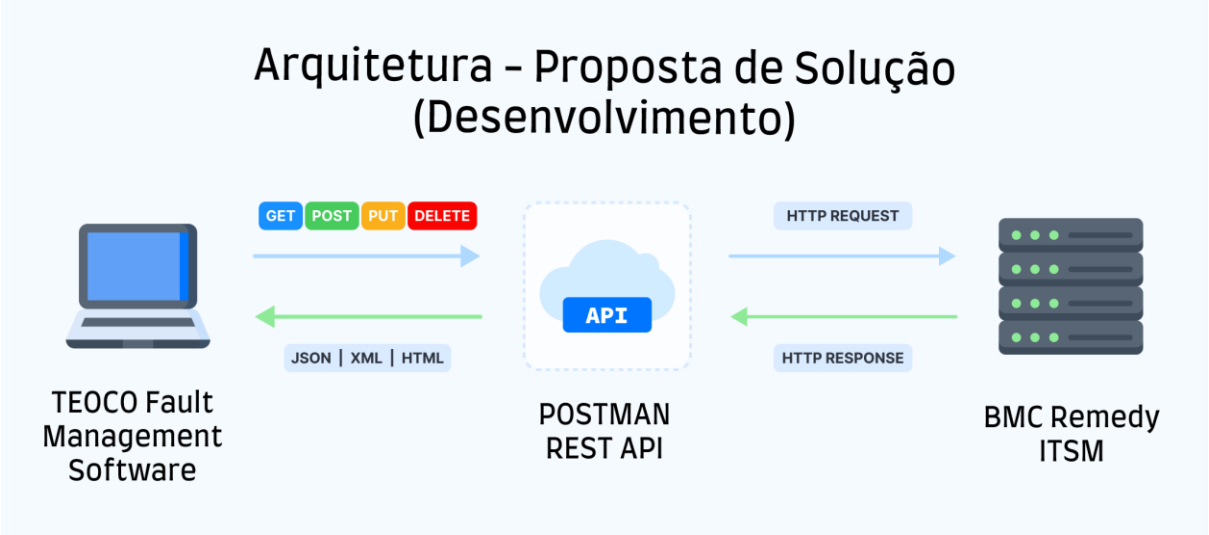


Figura 15: *Modelo da arquitetura da proposta de solução, desenhado em REST API. - Desenvolvido pelo autor, editado de: https://appmaster.io/pt/blog/o-que-e-a-api-rest-e-como-ela-difere-de-outros-tipos*

A proposta de solução assenta-se em três plataformas, conforme definido pela Figura 14:

• **TEOCO Fault Management**: Esta plataforma atua como o "Managing Server" no SNMP, e como "Client" na arquitetura REST. Por meio dela, há a disposição da alarmística que é apresentada para o operador NOC. Em seu estado atual, através da alarmística apresentada, o técnico do NOC valida a existência do incidente, e cria o ticket manualmente. A proposta de solução busca, através do estado do alarme, ou seja, se está ativo, criar o registo do incidente (ticket) automaticamente, e uma vez que o alarme desativar, realizar o fecho o incidente. Ou seja, na arquitetura, a plataforma será responsável por pedir requisições à plataforma ITSM, e fornece os dados, por meio de um HTTP Request, para o preenchimento do registo do incidente (nomeadamente, o nome do equipamento e o alarme).

O workflow da proposta de solução define-se quando um alarme ficar ativo, na plataforma da TEOCO Fault Management, há um *HTTP request (POST)*, em JSON, automaticamente, para a plataforma o BMC Remedy ITSM, no qual o Postman REST, permite a integração entre as duas plataformas. Uma vez que é enviado o *HTTP request (POST)*, há a criação do registo do incidente em BMC Remedy. Quando o estado da alarmística alterar, ou seja, quando o alarme não estiver mais ativo, o TEOCO Fault Management realiza outro *HTTP request* (*PUT*), em JSON, para a BMC Remedy ITSM, desta vez para atualizar e finalizar o registo de incidente.

• **BMC Remedy (ITSM)**: Uma das principais plataformas de ITSM, será responsável pelo registo dos incidentes, através dos tickets, e atua como "Servidor" na arquitetura REST, uma vez que transmite os dados ao "Cliente" (TEOCO Fault Management). Atualmente, a criação do ticket é manualmente, realizada pelo operador NOC, e a proposta de solução busca automatizar este processo. Com os dados recebidos pelo cliente, a plataforma, por meio do Postman REST API, será responsável pela criação e registo do incidente.

• **Postman REST API**: Postman é uma plataforma para criação e utilização de APIs. A proposta de solução busca integrar esta plataforma para preencher a categorização dos tickets criados no BMC Remedy, e criá-los, através do método POST, sem a intervenção humana, somente ao buscar o estado da alarmística, e finaliza-los através do PUT.

5 Desenvolvimento e avaliação

Conforme indicado anteriormente, a proposta de solução é uma estruturação do modelo de automatismo do Network Operations Center. Portanto, este capítulo busca tanto como estruturar e indicar o modelo de desenvolvimento, e também, indicar as métricas de validação da solução, uma vez que a solução não será efetivamente implementada e consequentemente, não haverão dados para a sua avaliação. A classificação será através de um questionário aplicado a dois operadores dos NOC (Coordenador e Gestor de Incidentes), que consiste em apresentar os benefícios da solução, bem como as principais dificuldades enfrentadas.

5.1 Postman REST API

A BMC possui documentação, através do Postman REST API, que permite o auxílio e integração para desenvolvimento de aplicações (Integrating ITSM with third-party applications by using the REST API), com tópicos que permitem criar, modificar e retirar informações de um registo de incidente. O âmbito da proposta de solução desenvolve-se através da criação e finalização do registo de incidente em BMC Remedy ITSM, por meio do Postman REST API e do estado da alarmística disposto em TEOCO Fault Management. A Figura 16 demonstra o ambiente da plataforma Postman API.

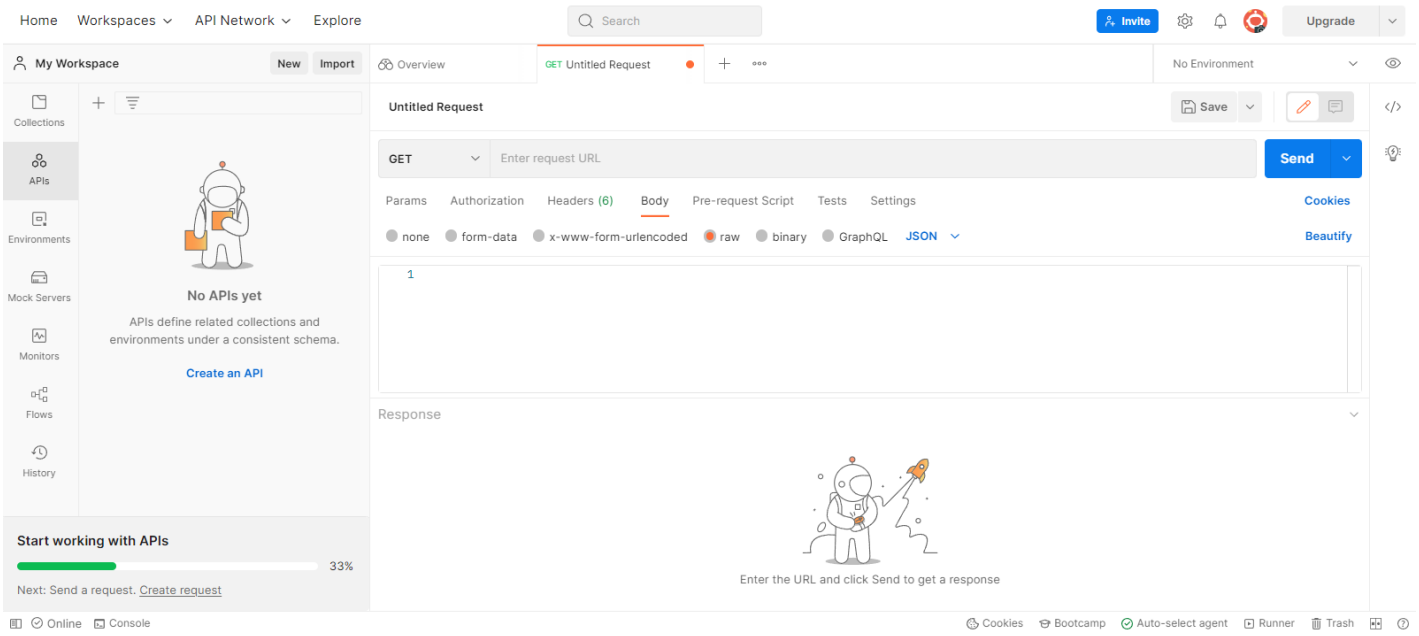


Figura 16: *Ambiente de desenvolvimento em Postman API. - Realizado pelo autor.*

Conforme descrito pela Postman em "Sending Requests", são definidos alguns requisitos para desenvolver e realizar *HTTP requests* pela plataforma. Cada request enviado pelo Postman necessita de uma URL que representa o *endpoint* da API que está a ser desenvolvida. A BMC, em sua documentação de suporte para desenvolvimento para criação do registo de incidentes, "Example of using the REST API to create an incident entry", indica para definir o *Request URL* através do URL:

```
http://serverName:port/api/arsys/v1/entry/HPD:IncidentInterface_Crea
te?fields=values(Incident Number).
```

O prefixo "serverName" define o local do ambiente de desenvolvimento, como por exemplo, "localhost". O prefixo "HPD:IncidentInterface_Create" é uma referência definida pela documentação da BMC em "The REST API references", que permite a criação de um registo de incidente.

Ao lado do "Request URL" são dispostos os diferentes métodos para *HTTP Request*, como GET, PUT, POST, PATCH, DELETE, COPY, contudo, no âmbito da proposta de solução, só serão utilizados os métodos: POST, responsável pela criação do registo de incidente, e o PUT, responsável pela alteração e finalização do registo de incidente.

O menu "Authorization" é responsável pela criação do token para autenticação do utilizador, para garantir segurança. O menu "Headers" permite com que seja enviado metadados importantes para o cumprimento da operação pretendida, por exemplo, antes de realizar a criação do incidente, é necessário realizar a autenticação do utilizador, para que não haja quebras de segurança.

O menu "Body" permite especificar os dados necessários para realizar o request. Há diversos formatos para definir como os dados serão enviados, por exemplo: form-data, binary, GraphQL, além do formato *raw*, que permite o desenvolvimento em JavaScript, HTML, XML e por fim, JSON, o formato sugerido pela BMC para o desenvolvimento.

Para o desenvolvimento da proposta de solução, é necessário cumprir todos os requisitos citados, e uma vez bem preenchidos, basta realizar o SEND, para que seja efetuado o request. Novamente, a proposta de solução passa por realizar este procedimento automaticamente,

através da verificação do estado da alarmística. Uma vez que o alarme estiver ativo, será realizado um *HTTP request (POST)*, no qual, os conteúdos que constam no Request URL, Authorization, Headers, e, parte do que consta no "Body" serão padronizados, uma vez que são incidentes reincidentes. O registo e finalização do incidente terá o equipamento que está "em alarme", e o seu envio por meio do Postman (SEND) será efetuado automaticamente, uma vez que todos os requisitos anteriores forem cumpridos, como a autenticação e categorização do "Body".

5.1.1 Criação do registo de incidente

Para iniciar o processo de criação de incidente, o cliente (TEOCO Fault Management Software) tem a opção da criação de incidente quando o estado da alarmística é alterado, contudo, é necessário o processo de criação da API. Portanto, com as alarmísticas pré-definidas, é determinar: alarme ativo (STATE = YES) inicia processo de criação do registo de incidente, alarme não ativo (STATE = NO), inicia processo de finalização do registo de incidente. Mas como é realizado a criação no Postman API?

A BMC, em sua documentação: "Example of using the REST API to create na incidente entry" e em "How to create new Incident ticket through REST API", descreve os passos necessários para a criação do registo de incidente. Inicialmente, deve-se definir o Request URL:

```
http://serverName:port/api/arsys/v1/entry/HPD:IncidentInterface_Crea
te?fields=values(Incident Number)
```

O "serverName:port" é o ambiente de desenvolvimento a ser criado, e o Incident Number é automaticamente atribuído após que o processo é terminado, ou seja, quando um registo é devidamente criado, e a referência "HPD:IncidentInterface_Create" é pré-estabelecido pela BMC para integração com "third-party applications". Além disso, é atribuído um token aleatoriamente, disposto nos "Headers", como uma *key* de "Authorization".

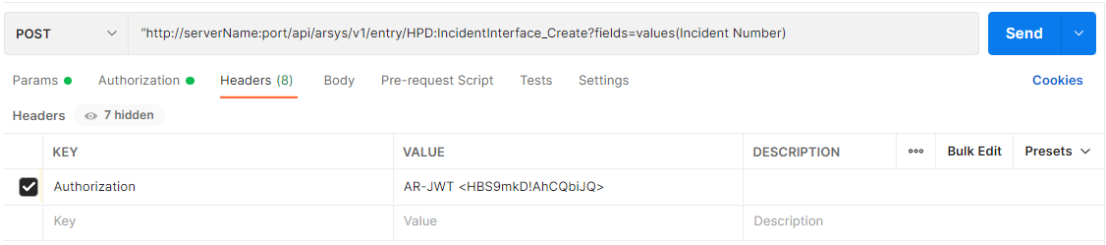


Figura 17: *Exemplo de desenvolvimento para criação de incidente na plataforma Postman API. - Realizado pelo autor.*

Posteriormente, no menu "Body", é definido o formato "raw", para se desenvolver em JSON. Em JSON, são estabelecidos os dados necessários para complementar o registo (input), ou seja, os campos que necessitam de ser previamente preenchidos na plataforma BMC Remedy (ITSM), conforme disposto na Figura 17. Uma vez que a proposta de solução é para incidentes reincidentes e sem impacto, ou seja, alarmes definidos como "Minor", o valor do campo "Impact" é o "4-Minor/Localized", com "Urgency: 4-Low". Esses valores são pré-estabelecidos pela plataforma BMC Remedy. Importante ressaltar que a configuração e envio da alarmística é realizado pelo fornecedor dos equipamentos de rede, ou seja, todos os alarmes dispostos no Managing Server para atuação do NOC foram previamente definidos pelos fornecedores dos equipamentos.

Figura 18: *Exemplo dos dados para preencher o registo de incidente em Postman API. - Realizado pelo autor.*

Dessa forma, o registo de incidente será criado, e será necessário atribuir à equipa necessária para resolução do incidente. A documentação da BMC, "The REST API references", com o host (Request URL):

```
http://serverName:port/api/arsys/v1/entry/TMS:TaskInterface
```

Através da URL e com o método POST, será adicionado uma "TASK", que permite encaminhar o incidente para quem de direito (2ª linha ou equipa de terreno). A referência "TMS:TaskInterface" é pré-definida pela BMC, e é utilizada para criação de TASK. Além disso, deverá ser o mesmo token de criação de incidente, para realizar a autenticação e prosseguir com os restantes passos. No menu "Body", em JSON, serão definidos os valores para preencher a criação da TASK, conforme apresentado na Figura 18.

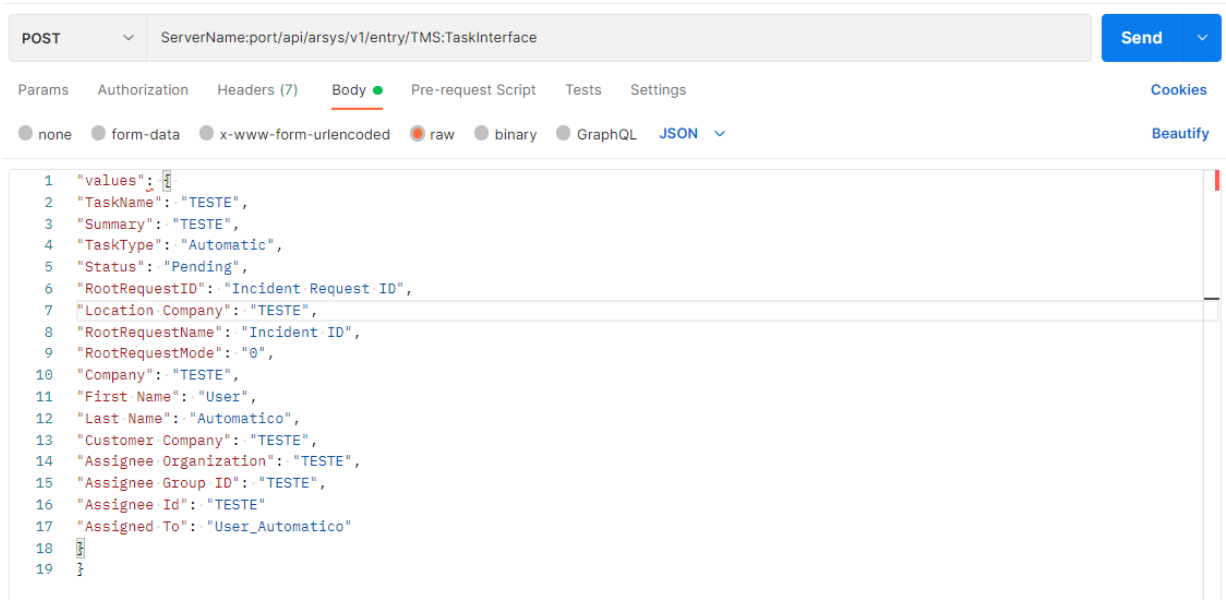


Figura 19: *Criação de TASK pelo Postman API. - Realizado pelo autor.*

Os valores nos quais está escrito "TESTE", serão previamente determinados pela equipa de desenvolvimento, e o "Incident ID" é determinado quando há a criação do incidente. Conforme apresentado no questionário, a plataforma cliente (TEOCO Fault Management) possui suporte para realizar os processos automaticamente pelo estado da alarmística.

5.1.2 Finalização do registo de incidente

Uma vez que a alarmística não estiver mais ativa, ou seja, quando o equipamento retorna ao seu estado inicial, inicia-se o processo de finalização do incidente. Para finalizar o incidente,

deverá fechar primeiro a "TASK" (2ª linha ou equipa para validação no terreno). Por meio do método PUT, na mesma Request URL para criação de TASK, é alterado o seu estado e assim, concluí-la, conforme ilustrado na Figura 19:

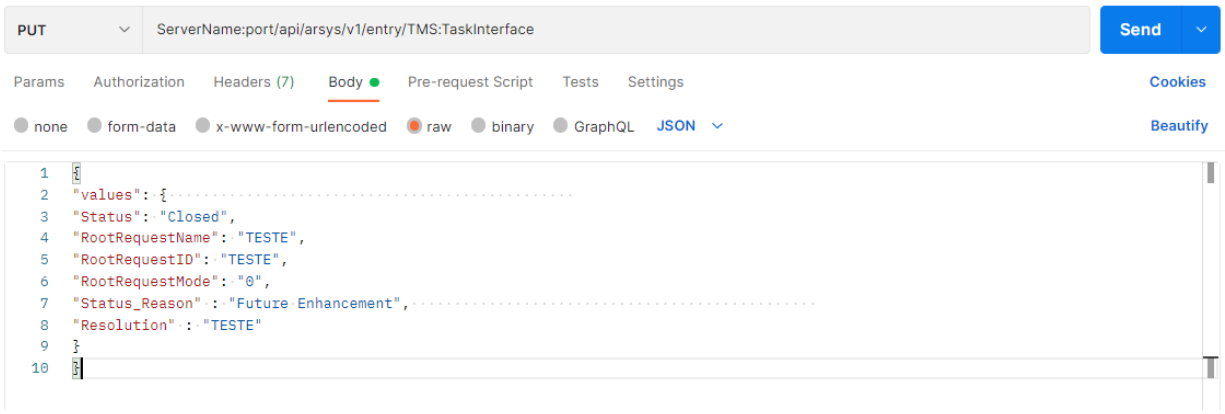


Figura 20: *Finalização da TASK pelo Postman API. – Realizado pelo autor.*

Para finalização do registo, o processo é similar, através do seguinte Request URL, e do método PUT:

```
http://serverName:port/api/arsys/v1/entry/HPD:IncidentInterface/RequestIDOfAnIncidentOnHPD:IncidentInterface
```

A referência "HPD:IncidentInterface" é previamente definida pela BMC, e é utilizada para pesquisar, ler e alterar um incidente que já foi criado, conforme descrito na documentação da BMC: "The REST API references". A referência no Request URL: "RequestIDOfAnIncidentOnHPD:IncidentInterface" busca automaticamente o ID do incidente referido, para realizar as devidas alterações. A Figura 20 apresenta os campos necessários para preenchimento.

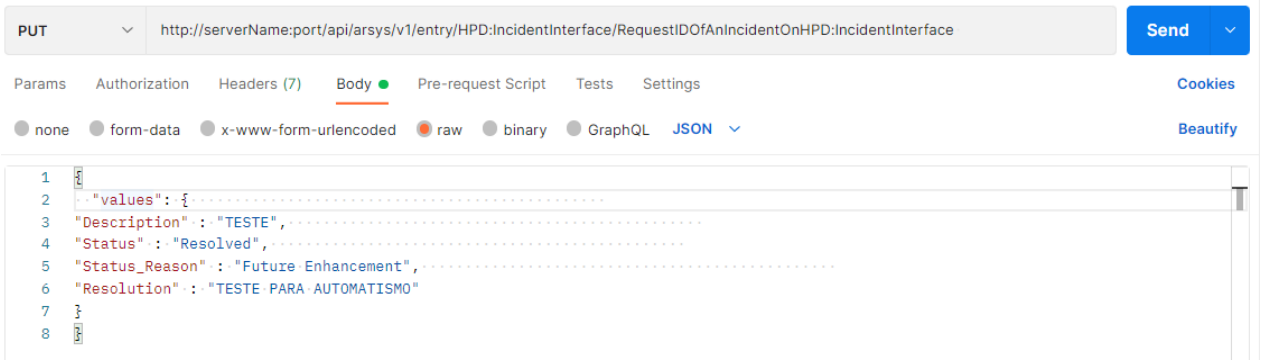


Figura 21: *Processo para finalização do registo do incidente. - Realizado pelo autor.*

5.2 Formulação da avaliação da proposta de solução

Conforme indicado anteriormente, a proposta de solução não foi efetivamente aplicada em ambiente de produção no ISP analisado, sendo assim, não é possível validar as suas funcionalidades e sua aplicação. Contudo, foi formulado um questionário à dois colaboradores do ISP, com objetivo de avaliar o formato da estruturação da proposta de solução, bem como todos os seus elementos, além de avaliar o estado atual do NOC, para que a sua implementação esteja bem definida. Um entrevistado atua na Coordenação do NOC, e o outro, trabalha como um Gestor de Incidentes no NOC. A descrição, apresentação dos objetivos do questionário e as perguntas realizadas estão dispostas no "Apêndice – Questionário NOC". O inquérito está definido em quatro classes, sendo que as classes A, B e C (Plataformas atuais; Eficiência do NOC; Follow-up de incidentes) buscam avaliar o estado inicial do NOC analisado, e a classe D (Analise da produtividade e eficiência do modelo proposto) irá determinar as expetativas de cada colaborador com o modelo proposto.

Para avaliar a proposta de solução apresentada em teor de produção, será necessário compreender o estado atual (AS IS), bem como o estado final (TO BE), e assim, analisar os seus resultados através de KPIs pré-estabelecidos, citadas abaixo. *Key Performance Indicators* (KPI) são utilizados para suporte no gerenciamento de um serviço, plano, projeto ou qualquer outra atividade de TI elegível a ser controlada e monitorada. Tem como objetivo a obtenção de Fatores Críticos de Sucesso. (AXELOS, 2020).

Conforme estabelecido anteriormente, a proposta de solução busca atuar em incidentes reincidentes e sem impacto, para permitir que o operador NOC possa direcionar a sua atuação em incidentes que verdadeiramente impactam o utilizador final. Para analisar o estado de

solução, é necessário compreender métricas que existem no estado atual, e comparativamente, aplica-las na proposta de solução, além de solucionar questões de implementação. Uma métrica é uma avaliação rotineiro que tem a função de comparar, dentro de um período, as informações produzidas e que geralmente são provenientes de um processo, serviço ou atividade (COHEN, 2015). As seguintes métricas foram adquiridas para análise da proposta de solução pelo questionário:

• Tempo de criação de ticket: quanto tempo leva, o operador NOC, uma vez que o alarme está ativo, para realizar o seu registo de incidente (ticket).

• Tempo de fecho de ticket: qual o tempo médio que o operador NOC necessita, uma vez que o alarme não está ativo, para validar o fecho do incidente.

• Percentagem de incidentes resolvidos pelo NOC: qual a percentagem de incidentes que são solucionados único e exclusivamente pelo operador NOC? Qual a quantidade de incidentes que são solucionados antes de terem impacto para o cliente final? O tratamento mais eficaz de incidentes sem impacto, permitem que incidentes não sejam escalonados com maior frequência, garantindo menos impacto para o utilizador final de rede.

• Cumprimento de RTO em SLA: conforme citado anteriormente, para a resolução de incidentes, são estabelecidos RTOs (Recovery Time Objectives) que devem ser cumpridos através do SLA (Service-Level Agreement). Qual a taxa de cumprimento médio de SLA para os incidentes? Ou seja, qual é o tempo médio de resolução de incidentes dentro do tempo estabelecido?

• Percentagem de chamadas perdidas: uma das principais funções de um técnico NOC é dar suporte especializado ao terreno, para a resolução de avarias. Portanto, com a quantidade de atividades do NOC, qual é a percentagem de chamadas que são perdidas?

• Quantidade de tickets com baixo impacto criados: comparativamente, qual é a quantidade de tickets que se encaixam na proposta de solução foram criados no último mês?

• Quantidade de tickets com impacto criados: a proposta de solução busca diminuir o tempo de atuação para incidentes de impacto final ao utilizador, ou seja, para que haja um registo de incidente mais rapidamente, para que a sua atuação também seja mais eficiente. Portanto, é

importante compreender a quantidade de ticket com impacto criados, para posteriormente, comparar com a proposta de solução.

• Follow-up de incidente com impacto: a proposta de solução permite que os operadores NOCs consigam ter maior follow-up de incidente com impacto, e assim, tornar a sua solução mais previsível e eficiente.

Além das plataformas, nas quais a solução será estruturada, ou seja, desenvolvida e implementada; as métricas, o que permite a comparação do estado atual com os objetivos que buscam ser alcançados pela solução, além de compreender a viabilidade da proposta, será realizado um questionário, conforme citado anteriormente, para dois colaboradores que atuam na área de uma das principais organizações que contam com um Network Operations Center de Portugal, mas que ainda utilizam um NOC sem automatismos. Através do inquérito, uma vez que o sistema não está implementado, os colaboradores são capazes de avaliar o modelo do atual do NOC, avaliar a estrutura da proposta de solução e estipular a sua eficiência do modelo proposto, uma vez que diversos processos manuais foram extintos do fluxo de trabalho do operador NOC.

6 Demonstração e Comunicação de Resultados

Conforme descrito no Subcapítulo 5.2, foi apresentado o questionário disposto no Apêndice "Questionário NOC" para dois atuantes em um Network Operations Center: o primeiro como um coordenador do NOC, atuante na área por 21 anos, e o outro, como um Gestor de Incidentes, atuante por 8 anos. O questionário é disposto em 4 partes essenciais: "Plataformas atuais" – busca compreender a escolha das plataformas para o desenvolvimento -, "Eficiência do NOC" – busca analisar a capacidade de trabalho do NOC, com os KPIs associados -, "Follow-up de incidentes" – pretende descrever a capacidade do NOC, consegue acompanhar a resolução dos incidentes que acontecem na rede – e por fim, "Analise da produtividade e eficiência do modelo proposto" – propõe compreender os benefícios da proposta de solução -.

No primeiro tópico "Plataformas atuais", compreende-se que a escolha se deve pela capacidade da flexibilidade, disponibilidade, escalabilidade e componentes de correlação de ambas as plataformas (TEOCO Fault Management Software e BMC Remedy). Ou seja, ao adquirir mais softwares com os fornecedores, é possível ter suporte para automatismos, de forma a potencializar o trabalho, contudo, a proposta da empresa é desenvolvê-las internamente, com o suporte das plataformas, uma vez que são escaláveis.

A "Eficiência do NOC" foi caracterizada conforme esperado, a equipa do NOC, com as diversas tarefas, possui bons números, mas que podem ser melhorados. O NOC possui uma taxa de chamadas perdidas de 6%, além do cumprimento médio de SLA, ou seja, quando um incidente é solucionado dentro do tempo estabelecido, de 92%. Valores que poderiam ter um maior cumprimento, caso os operadores NOC tivessem um menor fluxo de trabalho. Além disso, na pergunta B.10: "O NOC é independente para fechar tickets dos incidentes? Ou o fecho é solicitado por terceiros (2ª linha, equipa parceira, coordenação)?", foi indicado que o NOC tem a autonomia, contudo, em horários com maior fluxo de serviço, não conseguem dar seguimentos nos incidentes que estão a decorrer, e, portanto, grande parcela dos incidentes tem o pedido de finalização pelas outras equipas de operação ou pelas equipas parceiras. A proposta de solução busca diminuir a quantidade de chamadas não atendidas, e também, aumentar o cumprimento do SLA, além de aumentar a criação de tickets, e de permitir a melhoria da capacidade de gestão de incidentes pelo NOC. A Tabela 2 expõe os dados adquiridos por meio do questionário referentemente à eficiência do NOC atual. É a partir dos dados recolhidos, que

os colaboradores conseguem definir a expectativa do desempenho da plataforma proposta, e futuramente, uma vez que a proposta de solução estiver implementada, garantir comparações com a atuação do NOC de forma manual, e assim, validar efetivamente a solução.

Dados sobre a "Eficiência do NOC"		
Métricas	**Valores atuais**	**Valores esperados pelos colaboradores**
Tempo médio de criação de ticket	03 minutos.	Garantir que o tempo seja reduzido, uma vez que grande parcela dos tickets serão criados automaticamente.
Tempo médio de resolução de incidentes	Variável consoante o tipo de incidente: **Crítico** – 2 a 4 horas; **Urgente** – 4 a 24 horas; **Sem impacto**: 24 horas a 6 meses.	Os colaboradores esperam que a proposta de solução garanta uma eficiência de **70%**, comparativamente aos tempos atuais de resolução dos incidentes.
Percentagem de incidentes solucionados pelo NOC de forma independente	40%.	Os colaboradores esperam que a proposta de solução garanta uma eficiência de **65%.**
Taxa de cumprimento médio de SLA	92%.	97%.
Percentagem de chamadas perdidas	6%	Entre 2% e 1%.
Quantidade de tickets criados com impacto no último semestre	89.000 tickets, entre indisponibilidade	Não é possível mensurar, mas prevê-se uma redução da quantidade, uma vez

	total, parcial e degradação de serviço.	que o NOC terá um direcionamento para este tipo de incidentes.
Quantidade de tickets criados sem impacto no último semestre	51.000 tickets.	Não é possível mensurar, mas prevê-se um aumento da quantidade, uma vez que o automatismo irá tratar e solucionar de incidentes que antes não eram registados pelo NOC.

Tabela 2: *Dados recolhidos pelo questionário referente à "Eficiência do NOC". - Realizado pelo autor.*

O bloco "Follow-up de incidentes" permitiu compreender que o NOC é instruído para, em situações de maior impacto, solicitar "pontos de situação", isto é, informações sobre a resolução de incidentes, de 30 em 30 minutos, mas que pelo fluxo de trabalho, pode variar, até 45 minutos. A proposta de solução busca cumprir os 30 minutos previstos, uma vez que irá reduzir a carga de trabalho do NOC consideravelmente, apesar de não implementado, mas pela experiência de análise dos entrevistados.

Por fim, o bloco de perguntas "Analise da produtividade e eficiência do modelo proposto", permitiu compreender os benefícios da proposta de solução, analisada por ambos atuantes em um Network Operations Center. Por exemplo, a resposta D.8, foi caracterizada pelo Coordenador do NOC: "Além de nos dar uma noção mais objetiva da realidade, a criação de uma série de processos associados a automatismos, permite à Equipa passar a conseguir alocar mais tempo e recursos a outro tipo de funções de controlo da atividade, qualidade da entrega e desempenho global da Equipa." Além disso, caracterizam uma melhoria de desempenho de 80% para o mesmo tipo de tarefas, realizadas anteriormente de forma manual pelo NOC. O Gestor de Incidentes, caracterizou a pergunta D.7 como: "Com a implementação, busca-se ter uma ideia mais concreta dos reais problemas de rede, através dos casos tratados pelo automatismo proposto, devido ao aumento considerável das ocorrências detetadas/registadas", o que é um dos principais objetivos da proposta de solução, permitir que o NOC tenha uma perceção maior dos incidentes que estão a decorrer na rede. Perante a limitação de desenvolvimento, o principal método de avaliação são as respostas adquiridas pela experiência dos colaboradores em questão, pela a qual garantiram âmbito positivo.

7 Conclusões

Durante o desenvolvimento do estudo, foi possível definir as diversas práticas para o cumprimento do objetivo principal: a estruturação de modelo para um sistema de gestão da atividade de um NOC, para que haja maior eficiência processual e analítica.

Através da revisão da literatura, foi possível identificar os problemas atuais, revisados no questionário, e assim, estruturar e implementar toda a proposta de solução nos capítulos 4 e 5. A estruturação tem como requisitos: compreender o estado atual, identificar e solucionar a problemática apresentada, através dos processos ITIL e das ferramentas aplicadas, de forma a integrá-las para cumprir o objetivo principal do trabalho. Na implementação, a proposta de solução demonstrou-se apta para o cumprimento do objetivo proposto, aplicadas pela ferramenta proposta para a interligação do BMC Remedy e da TEOCO Fault Management Software, através do Postman API, avaliadas pelas métricas definidas no capítulo 5, e posteriormente, dispostas no capítulo 6.

O capítulo 6, por meio dos questionários aplicado aos colaboradores da organização, é possível concluir que a solução proposta capacita o aumento da produtividade do Network Operations Center. O automatismo dos incidentes de menor impacto, possibilita, pelo entrevistado, uma noção mais objetiva da realidade e alocação mais tempo e recursos a outro tipo de funções de controlo da atividade, qualidade da entrega e desempenho global da equipa, além de uma ideia mais coesa dos reais problemas de rede, através dos casos tratados pelo automatismo proposto, devido ao aumento considerável das ocorrências detetadas/registadas. Grande parte da implementação da solução, passa por toda a estruturação e definição do projeto, apresentada no capítulo 4, também avaliada positivamente pelos colaboradores. Ou seja, através da avaliação dos entrevistados por meio do questionário apresentado, a proposta de solução cumpre o seu objetivo principal de diminuir a quantidade de trabalho de um operador de um NOC, além de outros benefícios, como permitir com que o Network Operations Center direcione o trabalho para incidentes com maior impacto para o utilizador final, permitir maior eficiência na resolução de incidentes. Além disso, o trabalho apresenta escalabilidade de desenvolvimento, através das plataformas referidas, conforme indicado no questionário, contudo, serão tangíveis uma vez que implementado, pois estas não foram possíveis ser desenvolvidas no âmbito da proposta, mas que foram identificadas e apresentadas como trabalho futuro.

8 Limitações

Uma das maiores limitações da proposta de solução foi a ausência da utilização das plataformas para o desenvolvimento da solução. As plataformas mais relevantes, como a TEOCO Fault Management Software e o BMC Remedy ITSM, são disponibilizadas diretamente para organizações, seja a versão para desenvolvimento, seja a versão final, o que dificulta a visualização da proposta e também, a sua implementação. Consequentemente, um dos principais trabalhos futuros para progredir o trabalho, está em implementar a solução de forma definitiva. Além disso, outras limitações irão surgir durante o desenvolvimento do software, mas se espera, através da estrutura indicada, reduzir o máximo de questões de desenvolvimento, para que a sua implementação seja mais coesa e eficaz.

A acessibilidade do Postman API é um ótimo benefício, contudo, uma vez que não há acessos para as plataformas citadas, dificultam compreender o espetro de implementação da proposta de solução, pois não é possível determinar requisitos específicos que só aparecem durante o seu desenvolvimento. Durante o questionário apresentado aos atuantes em um Network Operations Center, há a confirmação que ambas as plataformas, possuem a capacidade de escalabilidade e flexibilidade, com ferramentas que auxiliam no desenvolvimento da solução proposta, contudo, sem a sua utilização, para desenvolver, prejudica o progresso e compreensão da proposta de solução.

9 Trabalho Futuro

Conforme citado anteriormente, a proposta de solução apresentada tem como uma de suas maiores limitações a ausência de licenças e plataformas para implementar o projeto. E como trabalho futuro, o início do processo de implementação da solução, através das plataformas citadas, em um ambiente de teste e desenvolvimento controlado, dentro de uma organização que possui um NOC.

Além disso, o objetivo do modelo apresentado é, a partir das alarmísticas de menor impacto, que possuem o mesmo processo de trabalho, serem automatizadas através da interligação do Managing Server, que busca o estado do alarme, e do registo na plataforma de ITSM. Um próximo passo para maior atuação da solução, seria utilizar um modelo de suporte à decisão, em Machine Learning, para auxiliar em alarmísticas de maior impacto, um exemplo é o estudo de David Côte e Shervin Shirmohammadi (2021).

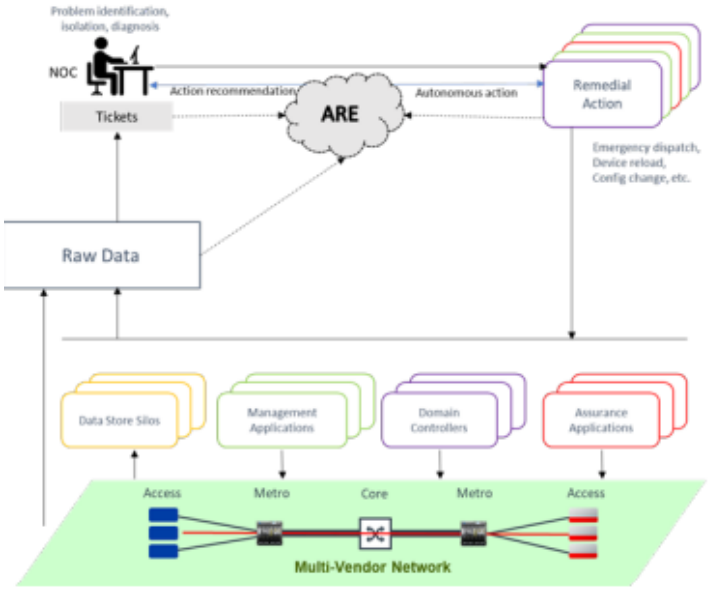


Figura 22: *Estrutura do NOC com o modelo de Machine Learning (ARE). Retirado de: "Automating Network Operation Centers with Superhuman Performance" (D. Côte & S. Shirmohammadi, 2021).*

A proposta, descrita na Figura 22, atua como um modelo de suporte à decisão, no qual o módulo ARE (Action-Recommendation Engine), através do Machine Learning e Reinforcement Learning, sugerir para o operador do NOC, qual a melhor atuação para resolução do incidente: "ARE utiliza dados, tickets e feedback de recomendações antigas para indicar

ações aos técnicos do NOC, ou para aplicar diretamente a solução.” ("Automating Network Operation Centers with Superhuman Performance”, D. Côte & S. Shirmohammadi, 2021).

Conforme indicado anteriormente, o NOC é responsável por gerir os incidentes da rede, e garantir que ela esteja em pleno funcionamento, de forma eficiente. Aliado do modelo proposto (Dispatching por alarmística básica), o módulo ARE permite gerir os recursos da rede com extrema eficiência, no qual o primeiro permite o tratamento de incidentes repetitivos e sem impacto direto para a rede, e o segundo, por meio do Machine Learning, indica a melhor solução para um incidente com maior impacto.

10 Referências Bibliográficas

Mauro, D, & Schmidt, K. (2001). *Essencial SNMP (1st Edition)*. California: O'Reilly.

Martins, R. et al. (2010, janeiro). *ITIL nas universidades: projecto-piloto em gestão de activos de TI no ISCTE-IUL.* [Sessão de conferência]. 10.ª Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI 2010). Lisboa. https://www.researchgate.net/publication/210365500_ITIL_nas_universidades_projecto-piloto_em_gestao_de_activos_de_TI_no_ISCTE-IUL

Kurose, J. & Ross, K. (2017) *Computer Networking: A top-down approach. (7th Edition).* Pearson Education.

Azasoo, J. & Boateng, K. (2015, junho). *A Retrofit Design Science Methodology for Smart Metering Design in Developing Countries.* [Sessão de conferência]. 5th International Conference on Computational Science and Its Applications (ICCSA). Canadá. DOI: 10.1109/ICCSA.2015.23

Peffers, K. et al. (2006). *Design Science Research Process: A Model for Producing and Presenting Information Systems Research.* [Sessão de conferência]. First International Conference on Design Science Research in Information Systems and Technology, California, Estados Unidos. https://arxiv.org/abs/2006.02763

Postman (s.d). *Building Requests.* https://learning.postman.com/docs/sending-requests/requests/

BMC (s.d). *Integrating ITSM with third-party applications by using the REST API*. https://docs.bmc.com/docs/itsm2102/integrating-itsm-with-third-party-applications-by-using-the-rest-api-974495994.html

Sousa, S. (2016). *Building a Network Operations Center (NOC) solution.* [Dissertação de mestrado]. UMA - Universidade da Madeira.

Mohammed, A. & Côte, D. (2021). *A Machine-Learning-Based Action Recommender for Network Operation Centers. IEEE Transactions on Network and Service Management, 18 (3), 2702-2713.*

AXELOS. (11 de janeiro de 2020). *Incident Management ITIL 4 Practice Guide*. AXELOS GLOBAL BEST PRACTICE.

Lucent Techologies. (22 de janeiro de 2001). *Network Operations Centers.* Network Industry Survey.

Externetworks. (s.d). *Network Operations Center.* https://www.extnoc.com/network-operations-center/

Rao, P. (1 de março de 2022). *NOC Performance Metrics: How to Measure and Optimize Your Operation*. INOC. https://www.inoc.com/blog/noc-metrics

Fielding, R. (2000). *Architectural Styles and the Design of Network-based Software Architectures.* [Tese de doutoramento]. Universidade de Califórnia.

Miloslavskaya, N. (2018). *Network Security Intelligence Center as a combination of SIC and NOC*. [Sessão de conferência]. 9th Annual International Conference on Biologically Inspired Cognitive Architectures. Praga, República Checa. DOI: 10.1016/j.procs.2018.11.084

COHEN, Roberto (2015). *Métricas para help desk e service desk: principais métricas de desempenho, seus usos e armadilhas nos pequenos e médios centros de suporte*. Novatec Editora.

Apêndice - Questionário NOC

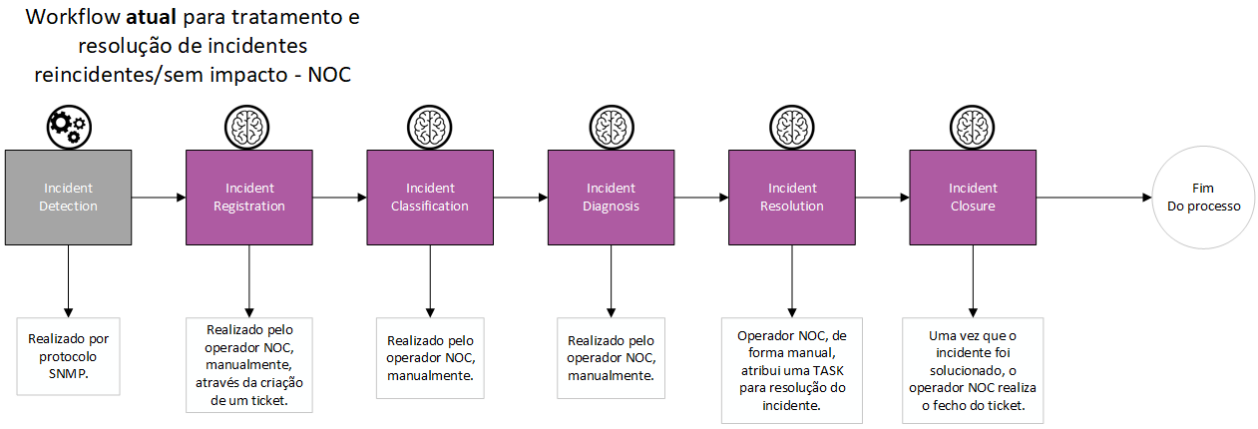
Entrevistado:

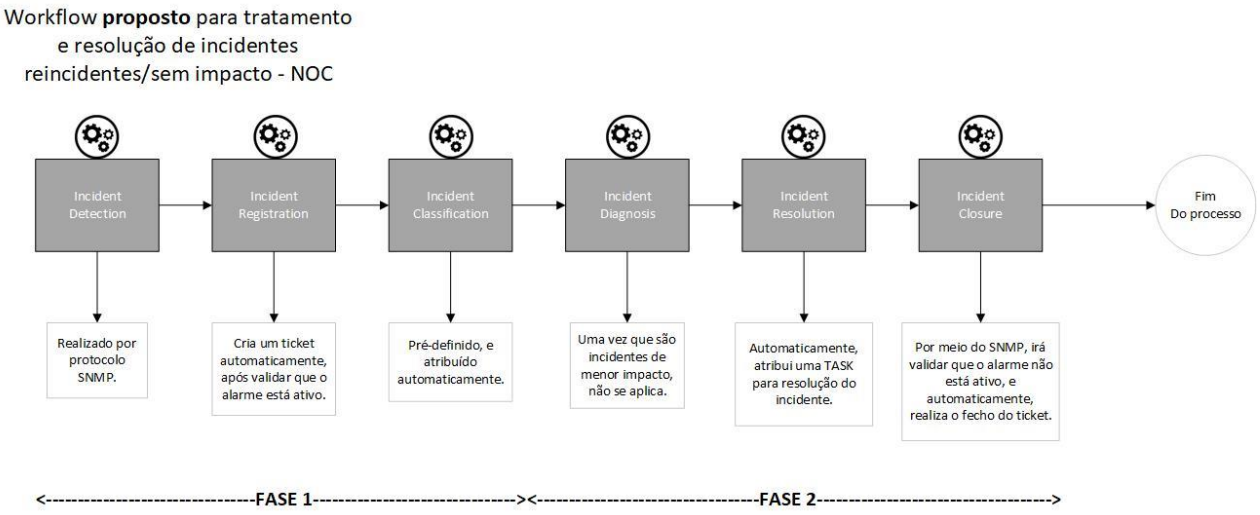
Categoria profissional:
Antiguidade na empresa:

Tema: Automatismo de incidentes sem impacto e reincidentes em um Network Operations Center.

Descrição inicial: O questionário busca avaliar o estado atual do Network Operations Center, principalmente a criação de incidentes reincidentes sem impacto de forma manualmente, bem como as consequências para o restante das vertentes do NOC. A proposta de solução, busca tratar os incidentes sem impacto automaticamente, através do TEOCO Fault Management Software (plataforma para disposição dos alarmes), BMC Remedy (ITSM) e de uma API (Postman REST API), que busca o estado do alarme para criar ou fechar um incidente. Segue abaixo, o estado inicial e o estado proposto para trabalho de incidentes reincidentes/sem impacto.

Para a implementação, em busca de identificar falhas processuais que poderão existir, propõe realizar em fases. A **fase 1** comtempla todo o processo de recolha da informação da alarmística e a criação do registo do incidente, com o auxílio do técnico do NOC para encaminhar para a equipa de resolução. Já a **fase 2** busca endereçar a equipa de resolução, seja uma 2ª linha ou uma equipa de resolução no terreno, e uma vez que o incidente está solucionado, finalizar a instância, completamente automaticamente. Uma vez que o *workflow* esteja em seu funcionamento indicado, os registos de incidentes reincidentes não comtemplarão a intervenção do NOC, sendo assim, realizado automaticamente. As figuras a seguir demonstram o estado atual para o tratamento de incidentes reincidentes/sem impacto, e a proposta de solução, caracterizada em duas fases.





Blocos	**Objetivos**	**Questões**	**Respostas**
A. Plataformas atuais	• Compreender quais são as plataformas utilizadas na organização; • Benefícios das plataformas utilizadas.	1) Qual é a plataforma de disposição de alarmística utilizada na organização? 2) Qual a plataforma de	1) 2) 3)

		ITSM utilizada na organização? 3) Quais as vantagens da plataforma mediante a outras do mercado? 4) As plataformas permitem escalabilidade? 5) A plataforma *TEOCO Fault Management* possui suporte para automatismos através do estado do alarme?	4) 5)
B. Eficiência do NOC	• Compreender o tempo de atuação dos técnicos do NOC, e o tempo de resolução de incidentes.	1) Qual o tempo médio que um técnico do NOC utiliza para criar um ticket?	1) 2)

	• Compreender a eficiência do NOC frente ao cumprimento dos SLAs estabelecidos. • Caracterizar a quantidade de tickets criados (seja com impacto, ou sem impacto).	2) Qual o tempo médio que um incidente fica "In Progress", ou seja, pendente de resolução? 3) Qual o tempo médio da resolução de incidentes? 4) Qual a percentagem de incidentes que são solucionados pelo NOC? Isto é, sem atuação de terceiros. 5) Qual a taxa atual do cumprimento médio de SLA? Ou seja, qual a tempo médio de resolução de incidentes dentro	3) 4) 5) 6) 7) 8) 9) 10)

		do tempo estabelecido? 6) Qual a quantidade de tickets com impacto que ultrapassam o SLA estabelecido? 7) Qual a percentagem de chamadas perdidas? 8) Qual a quantidade de tickets sem impacto criados no último semestre? 9) Qual a quantidade de tickets com impacto criados no último semestre?	

		10) O NOC é independente para fechar tickets dos incidentes? Ou o fecho é solicitado por terceiros (2ª linha, equipa parceira, coordenação)?	
C. Follow-up de incidentes	• Caracterizar a capacidade do NOC de seguir e acompanhar a resolução de incidentes com impacto (Incident Monitoring).	1) Com que frequência os operadores NOC são instruídos para pedir um ponto de situação de incidentes com impacto? 2) Qual a frequência atual do follow-up de incidentes com impacto?	1) 2) 3) 4)

		3) O NOC é independente para dar follow-ups em incidentes pendentes com impacto? Ou o follow-up é solicitado por terceiros (2ª linha, equipa parceira, coordenação)? 4) Qual a quantidade de incidentes que são resolvidos antes de serem escalados? Ou seja, antes de terem um impacto ao utilizador final.	
D. Analise da produtividade e eficiência do modelo proposto	• Estimar a diferença de produtividade do NOC, com a implementação do modelo proposto.	1) Qual a sua opinião sobre a implementação da fase 1? 2) Com a implementação da fase 1, quais	1) 2) 3)

		atividades do NOC tiveram mais contributo? 3) Qual a proporção (%) entre o tempo para cumprir as atividades na fase 1, comparativamente com o estado atual do NOC? 4) Qual a sua opinião sobre a implementação da fase 2? 5) Com a implementação da fase 2, quais atividades do NOC tiveram mais contributo?	4) 5) 6) 7) 8)

		6) Qual a proporção (%) entre o tempo para cumprir as atividades na fase 2, comparativamente com o estado atual do NOC? 7) Com a implementação finalizada, quais as métricas do NOC tiveram maior evolução (Ex.: quantidade de tickets criados; tickets que ultrapassam o SLA; chamadas perdidas; tempo médio de resolução de incidentes; etc)?	

		8) Qual o maior contributo do modelo proposto?	