RELATÓRIO TÉCNICO COM BASE EM ITIL

Uma aplicação de boas práticas em um centro de operações de segurança

Elaborador:	Tierre Amaral
Orientador:	Professor Edson Roberto Gaseta

Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS

Dados Internacionais de Catalogação-na-fonte

A516r AMARAL, Tierre

Relatório técnico com base em ITIL: uma aplicação de boas práticas em um centro de operações de segurança. / Tierre Amaral. – Americana, 2019.

42f.

Relatório técnico (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Edson Roberto Gaseta

1 Governança de sistemas de informação I. GASETA, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.519

Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

Tierre Amaral

RELATÓRIO TÉCNICO COM BASE EM ITIL

Uma aplicação de boas práticas em um centro de operações de segurança

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 5 de Dezembro de 2019.

Banca Examinadora:

Edson Roberto Gaseta
Professor
FATEC

Murilo Fujita
Professor
FATEC

Rogério Nunes de Freitas
Professor
FATEC

SUMÁRIO

Lista de figuras

Lista de tabelas

1 OBJETIVO DO RELATÓRIO TÉCNICO

Atualmente, as organizações buscam melhores resultados e formas de atender o mercado competitivo, empregando conceitos inovadores de melhoria contínua (DRUCKER, 2014).

Estas melhorias podem contribuir diretamente nas áreas empresariais, com o sistema de tecnologia da informação tem um papel essencial para garantir disponibilidade dos dados e interligação destas áreas através de sistemas inteligentes de informação, com a responsabilidade de interagir diversos setores e operações, transações e facilitar as operações dentro da empresa, de forma íntegra e padronizada vinda da área de TI (AGUTTER, 2013).

Diante deste conceito, diversas ferramentas auxiliadoras são utilizadas para facilitar a execução, como por exemplo as boas práticas de ITIL, voltada à entrega de serviços com processos estruturados e definidos, objetivando o alinhamento dos procedimentos e etapas de início até entrega do serviço, alinhando a comunicação de todas as áreas de TI e da organização, minimizando custos e otimizando processos. A otimização destes processos compõem etapas de melhoria contínua que podem ser aplicáveis em níveis de produção e suporte (AGUTTER, 2013).

Com base nestes estudos, cria-se o entusiasmo de apresentar um relatório operacional no qual todos os fatores teóricos e de boas práticas poderiam ser apresentados dentro de um ambiente de operação de atendimento de segurança da informação, estudando os processos e procedimentos que podem ser otimizados e trabalhados de modo a ampliar e definir escopos que agregam valor ao serviço e que refletem na satisfação do cliente. Estes mesmo que, quando aprofundados, observa-se uma real capacidade de análise de métricas e atual cenário que possa ser trabalhado para melhoria. Este cenário pode ser dividido em níveis de suporte, que quando detalhados, identificam-se tarefas as quais os níveis superiores de suporte possam delegar certas atividades para níveis inferiores, com a base e o objetivo de entrega de soluções mais rápidas para os clientes, foco de tarefas complexas maiores para os níveis superiores, padronização e documentação de processos e desenvolvimento técnico dos analistas.

2 DESENVOLVIMENTO

Para providenciar um relatório técnico com embasamento, entende-se que é necessário o estudo teórico do conceito de inovação e boas práticas de ITIL, para assim poder aplicadas dentro do ambiente de operações.

2.1 BASE TEÓRICA – FUNDAMENTOS DE INOVAÇÃO

Como embasamento teórico para o desenvolvimento do relatório, o conceito e estudo na inovação foi primordial. Para Drucker (2014, p. 190):

“A inovação é tanto conceitual como perceptual. […] inovação é portanto sair para olhar, perguntar, escutar. “

Entende-se que a inovação é portanto uma atitude de questionar e entender o porque que determinado processo, serviço, atividade ou produto é executado ou feito de uma forma, tentando identificar possíveis melhorias.

Ainda para o autor (2014, p. 191):

> “As inovações eficazes começam pequenas. Não são grandiosas. Procuram fazer uma coisa específica […].É melhor que as inovações começam pequenas, exigindo inicialmente pouco dinheiro, pouca gente, e somente um mercado pequeno e limitado”.

A partir da ideia de Drucker (2014), evidencia-se que a inovação não dependente de recursos grandiosos como financeiros ou processuais. Simples detalhes que melhoram e que possam ser incluídos em um produto já exalam a ideia principal de inovação e melhoria, possibilitando a mensuração do novo produto ou processo através de ferramentas de auxílio.

Segundo Adair (2007, p. s/p, tradução nossa):

> “Inovar significa, literalmente, trazer ou introduzir algo novo – alguma boa ideia, método ou dispositivo.[...] a inovação como um conceito mais amplo tem certas facetas importantes. Em particular, combina dois principais processos que se coincidem: ter novas ideias e implementá-las.”

Conclui-se devidamente que a inovação pode ser aplicada a diversas situações, combinando atitudes de mudar, melhorar e otimizar esses processos e fomentar a implementação de modo ágil e fácil, trazendo um diferencial a todo o negócio empresarial, como forma de maximizar ganhos e lucros na empresa.

O nível de ganho e reconhecimento dessas novas ideias e melhorias podem ser altos e diretamente relevantes para a organização, de modo a atrair visibilidade de altos níveis de executivos e investidores que concretizam e criam confiança perante a organização, mostrando o mercado-alvo e o momento de negócio que se diferencia dos demais concorrentes em competição da empresa.

2.2 BASE TEÓRICA – BOAS PRÁTICAS DE ITIL

Conforme reflexão dentro dos pensamentos apresentados dos autores, podemos aplicar a inovação e renovação de processos com base também em boas práticas, como o ITIL *(Information Tecnology Insfractructure Library).*

A ITIL surgiu do Reino Unido na década de 80. Durante todos estes anos, as boas práticas passaram por diversas mudanças e altos níveis de aprimoramento, que em 2007, passou por uma significativa mudança direcionando e focando nos desafios de tecnologia da informação atuais, passando sua versão três (Global Knowledge, 2011).

Segundo Agutter (2013, p. s/p, tradução nossa):

> "A ITIL recomenda o desenvolvimento de definições de serviços baseado em resultados. Isso quer dizer que nós precisamos analisar os resultados do cliente entregados pelo serviço, e não a tecnologia do serviço de TI que é oferecida para o cliente."

Para Magalhães e Pinheiro (2007, p. 64):

> "A ITIL é composta por um conjunto das melhoras práticas para definição dos processos necessários ao funcionamento de uma área de TI [...] com o objetivo permitir o máximo de alinhamento entre área de TI e as demais áreas de negócio, de modo a garantir a geração de valor à organização"

Diante da argumentação dos autores, pode-se entender que a ITIL é um guia de melhores práticas que objetiva a definição e estruturação da área e processos de TI junto a toda organização e seu negócio, agregando valor operacional e financeiro para a empresa. Definido por várias etapas e processos de melhoria, a ITIL deve ser desenvolvida e alinhada com os objetivos da TI, da empresa e do cliente, entendendo os resultados, serviços e entregáveis do cliente de modo que as tecnologias tanto de fornecedor quanto cliente possam estar em harmonia.

Atualmente há um alto crescimento nos níveis de complexidade, número de processos distintos de TI nas organizações assim como os desafios de implementação sem fazer grandes alterações que impactam o negócio e operações. A ITIL oferece um estudo

destes planos para manter a demanda de negócio e suas tecnologias, atuando no alinhamento estratégico da empresa (MILLS, VAN HOVE, 2013).

Perante esta definição, a ITIL pode ser considerada também como uma parte essencial para os processos da área de tecnologia da informação com ênfase no gerenciamento de serviços de TI. Ela demonstra as práticas que devem atender de forma otimizada as necessidades da organização, através do planejamento e gerenciamento dos serviços de TI, coligando os processos de perspectiva de negócio e tecnologia da informação.

De acordo com o autor Agutter (2013), a ITIL firma-se em cinco fases principais, cobrindo o ciclo de vida de um serviço do inicio ao fim, providenciando alto nível de guiagem de informação e processos. Estes volumes são designados como Estratégia de serviço, Desenho de serviço, Transição do serviço, Operação do serviço e Melhoria contínua do serviço. A figura 1 demonstra o ciclo do serviço, as estratégias e as boas práticas interligadas:

Figura 1 - Ciclo de Vida do Serviço

Baseado em Axelos (ITIL®) material. Reproduzido sob licença da Axelos.

Fonte: Axelos (ITIL®)

A Estratégia de serviço define qual o objetivo do prestador de serviço em relação da importância de seu negócio, quais os planos e decisões para atingir e satisfazer o cliente. De modo geral, propõe o entendimento do valor do serviço, define e opera as estratégias, gerencia e planeja os ativos e define relacionamentos para satisfazer e alcançar suas necessidades e sucesso, identificando os riscos e oportunidades (MILLS, VAN HOVE, 2013).

Entende-se a importância o planejamento e entendimento da estratégia de serviço por certificar e fortificar a missão da empresa e seus serviços, definir a operação e políticas para assim gerar a arquitetura do serviço e seu desenho em mais detalhes. Com isto, o Desenho de serviço mostra-se crucial para o sucesso dos entregáveis. Seu foco maior é desenhar os serviços, processos e procedimentos de alta qualidade, de forma que sua entrega funcione propriamente (AGUTTER, 2013).

Para Melo, Oliveira e Almeida (2017, p. 63):

> "O ciclo de Desenho de Serviço está inserido nesse contexto, pois, após a definição das estratégias no ciclo de Estratégia de Serviço, devem ser coletados requisitos para o desenho das soluções [...]. O Desenho de Serviço deve ser estruturado de modo que garanta a qualidade da prestação de serviços e, consequentemente, leve à satisfação do cliente".

Com a análise do esclarecimento de Agutter (2013) e a definição do Desenho de serviço dos autores Melo, Oliveira e Almeida (2017), conclui-se que o desenho de serviço é diretamente interligado à necessidade do cliente e estratégia da empresa, de forma a apresentar competitividade e controle de custo sem comprometer a qualidade do serviço. Conforme a racionalização da estratégia e desenho de serviço, a apresentação deste serviço é aplicado nos procedimentos de transição do serviço.

A etapa de transição de serviço constitui-se em trabalhar e garantir que o serviço esteja diretamente alinhado com o que foi planejado em sua estratégia e desenho. Deve ser trabalhada formas de que este serviço seja entregue com eficiência, com riscos mínimos e mitigáveis, identificando também as oportunidades de negócio (MELO, OLIVEIRA E ALMEIDA, 2017). A transição de serviços é a fase pela qual é trabalhada possíveis mudanças, analisando o que foi planejado contra o que já está em produção, de forma a diminuir a variância do que está em desenvolvimento e o que é real. É uma etapa significativa para acentuar quais os pontos críticos a serem trabalhados.

A partir da transição de serviços, entra-se no estágio da operação do serviço. De modo geral, a operação de serviço concebe na entrega do serviço devidamente planejado e

estudado detalhadamente visando um alto nível de qualidade e que suporte de forma acertiva as necessidades do negócio e clientes.

De acordo com Agutter (2013, p. s/p, tradução nossa):

“Clientes esperam o ambiente de operação estável e bem suportável, e ao mesmo tempo, esperam melhorias e pequenas mudanças que sejam implementadas rapidamente efetivamente para o negócio”.

Para Mills e Van Hove (2013, p. s/p, tradução nossa):

> “Operação de serviço tem como objetivo manter (melhorar) a satisfação do negócio e confidencialidade nos serviços de TI, minimizar impactos de interrupções que não podem ser prevenidos proativamente e garantir os que os serviços estejam acessíveis somente a aqueles que estão autorizados a utilizá-los”

Conforme a importância da operação de serviços para os autores, conclui-se que esta fase do ciclo do serviço deve ser enfatizada como um reflexo de todo o trabalho e estudo do planejamento do serviço, identificando soluções e melhorias, minimizando riscos e explorando oportunidades, de forma que novas implementações não impactam o cliente e apareçam de modo expressivo para as partes interessadas em caso de ganhos e vantagens para o serviço. Por outro lado, busca-se impacto zero ou mínimo possível, quando relacionados a resolução de problemas.

Conforme Global Knowledge (2016), dentro de operação de serviços concede diversas tarefas de gerenciamento, enfatizando o gerenciamento de requisição de serviço, incidentes e problemas, sendo detalhados da seguinte forma:

- Gerenciamento de Requisição de serviço: gerenciar as atividades, operações e pedidos do serviço, demonstrando controle, tempo de resposta ágil, qualidade e satisfação. É denominado como reflexo das operações para o cliente externo, cujo pretende-se mostrar valor, flexibilidade e dados que justificam o investimento ou serviço contratado pelo cliente.

- Gerenciamento de Incidentes: restaurar o serviço comprometido da forma mais rápida possível, mantendo as ferramentas e utilidades na mais alta disponibilidade reduzindo impactos e perdas.

- Gerenciamento de Problemas: identificar quais as causas raízes de incidentes ou rupturas ocorridas no serviço, enfatizando sua resolução e possíveis previsões.

Além deste fatores de gerenciamento Global Knowledge (2016), a operação de serviços conta com a importância da central de operação de serviço, definida como ponto focal e principal dos clientes para contatos de pedido de serviços e incidentes, sendo o maior ponto de comunicação e de grande responsabilidade para direcionar as atividades.

Com as descrições dos processos de gerenciamento e partes envolvidos para a etapa de serviço de operação, é primordial que o profissionalismo em pedidos seja efetivo, como é comportada na relação de requisições feitas por clientes ou usuários. Estas requisições seguem os padrões de gerenciamento de requisição de serviço.

De acordo com Global Knowledge (2016, p. 5-46, tradução nossa):

> "Requisição de pedido é um conjunto de processos genéricos que suprem pedido de serviços de usuários. Estes pedidos são frequentemente simples e de baixo custo, que podem ser apenas esclarecimento de perguntas. "

Segundo Mills e Van Hove (2013, p. s/p, tradução nossa):

> "Os objetivos das requisição de serviços é processar pedidos de forma efetiva e eficiente (exemplos: serviços, informação, reclamações, aplicações, etc) [...] providenciar mecanismos para agilizar solicitações e providenciar mecanismos efetivos de comunicação da informação sobre o estado de pedidos ... "

Enfatizando a definição e objetivo argumentada pelos autores, entende-se que o processo de requisição de serviços está diretamente interligado na satisfação do cliente e dos usuários. Garantir que uma solicitação de serviço ou pedido seja processada de forma eficiente de com alta responsividade são fatores reflexivos de qualidade. Estes pedidos podem ser variados, porém é imprescindível que sejam trabalhados de forma ágil e profissional nas atividades diárias.

Seu escopo contempla requisições e pedidos feitos diariamente por clientes internos e externos, que em alguns casos podem ser vinculados a incidentes (pedidos de mudanças para resolução de um incidente) ou pedidos simples, separados por categorias e organizados de forma prioritária (Global Knowledge, 2016).

Na continuidade da requisição de pedidos e a vinculação a incidentes, tanto clientes internos quanto externos podem reportar certas indisponibilidade de ferramentas, serviços ou acessos, que impactam diretamente nas operações e finanças. Estes incidentes devem ser tratados de forma competitiva e profissional, objetivando a minimização de prejuízos e reflexos de qualidade. Baseado nestes conceitos, enfatiza-se a importância do processo de gerenciamento de incidentes.

Um incidente pode ser denominado como uma interrupção não planejada de um processo ou serviço de TI, redução de qualidade deste serviço e até falhas de configuração de uma ferramenta, produto ou serviço que ainda não impactam diretamente as operações (Global Knowledge, 2016). Dada esta definição de incidente, a proposta de gerenciamento

de incidentes é de restaurar este serviço da forma mais rápida possível, com a responsabilidade de diminuir o tempo de indisponibilidade e impacto no negócio (Agutter, 2013).

Para Agutter (2013, p. s/p, tradução nossa), o gerenciamento de incidentes caracteriza-se com os principais objetivos:

- Garantir que métodos e procedimentos padrões sejam utilizados para otimizar o tratamento de incidentes
- Otimizar comunicação sobre incidentes para a coordenação de TI e negócio
- Otimizar a reputação de TI pelo gerenciamento profissional de incidentes
- Priorizar incidentes de acordo com as prioridades de negócio
- Manter a satisfação do cliente e usuário com a qualidade do serviço de TI.

Diante destes objetivos, o escopo do gerenciamento de incidentes é composto por qualquer evento ou acontecimento que indique um distúrbio em um serviço de TI reportados por clientes externos, parceiros ou usuários internos. Não fará parte do escopo eventos informativos que indicam serviços operacionais normais ou qualquer pedido ou requisição de serviço (Global Knowledge, 2016).

Com a problematização e entendimento do escopo, o processo de gerenciamento de incidentes é constituído por diferentes conceitos, como modelo de incidentes, escala de tempo de entrega e incidentes críticos. Com base nisto, a estrutura de um modelo de incidentes é fundamental para definição dos outros conceitos.

Este modelo de incidente tem como objetivo e termo pré-definir os passos que devem ser seguidos para tratamento de diferentes prioridades e tipos de incidentes. Este modelo segundo Global Knowledge (2016), deve conter:

- Os passos que devem ser seguidos para o tratamento de incidente
- A ordem cronológica destes passos, com qualquer dependência definida ou sub-processo.
- Responsabilidades e responsáveis
- Precauções que devem ser seguidas antes do início de resolução do incidente, como backup de dados, arquivos de configuração ou qualquer tipo de tratamento pré-resolução
- Processo de escalação, que deverá ser contactado e quando
- Qualquer atividade de preservação de dados e segurança

Para Agutter (2013, p. s/p, tradução nossa):

> “Dados e informação coletadas são particularmente importantes se o incidente for escalado para o segundo nível de suporte. Vários times de suporte reclamam do fato de não receberam informação suficiente, voltando assim o incidente escalado para o primeiro nível. Isso consequentemente regada em perda de tempo e faz com que o tempo de resolução aumente.”

Coligando as atividades do modelo de incidente conforme Global Knowledge (2016) e a importância de um processo de escalação bem definido segundo Agutter (2013), entende-se que a comunicação entre times de suporte e procedimentos definidos são vitais para evitar problemas durante a resolução de incidente e garantir finalização dentro do prazo estipulado. Conclui-se que há uma grande responsabilidade tanto em níveis iniciais quanto níveis superiores de suporte, que não devem ser tratados separadamente mas sim em conjunto refletindo um único time para os consumidores, dentro dos contratos segregados com os mesmos e na escala de tempo estipulada internamente.

Com o entendimento do processo de gerenciamento de incidentes, o processo de gerenciamento de problemas pode auxiliar na prevenção de possíveis incidentes no futuro.

Definido por Mills e Van Hove (2013, p. s/p, tradução nossa), a ITIL define como principais objetivos do gerenciamento de problemas:

- Prevenção de problemas e incidentes
- Eliminar incidentes recorrentes
- Minimizar impacto de incidentes que não podem ser prevenidos

O objetivo do gerenciamento de problemas é entender a causa de problemas e causas raízes, enfatizando a comunicação e documentação para auxiliar o time de suporte técnico com documentações e comunicação efetiva, e novamente de forma pró-ativa, prevenir possíveis incidentes futuros. Como escopo, o processo de gerenciamento de problemas está interligado a um ciclo de vida, coletando informações, gerenciamento investigação de causas e diagnóstico, aplicando procedimentos de mudanças caso necessário de forma reativa, identificando possíveis problemas de incidentes já registrados ou de forma pró-ativa, identificando melhorias que possam prevenir incidentes, utilizando diferentes ferramentas. (Agutter, 2013).

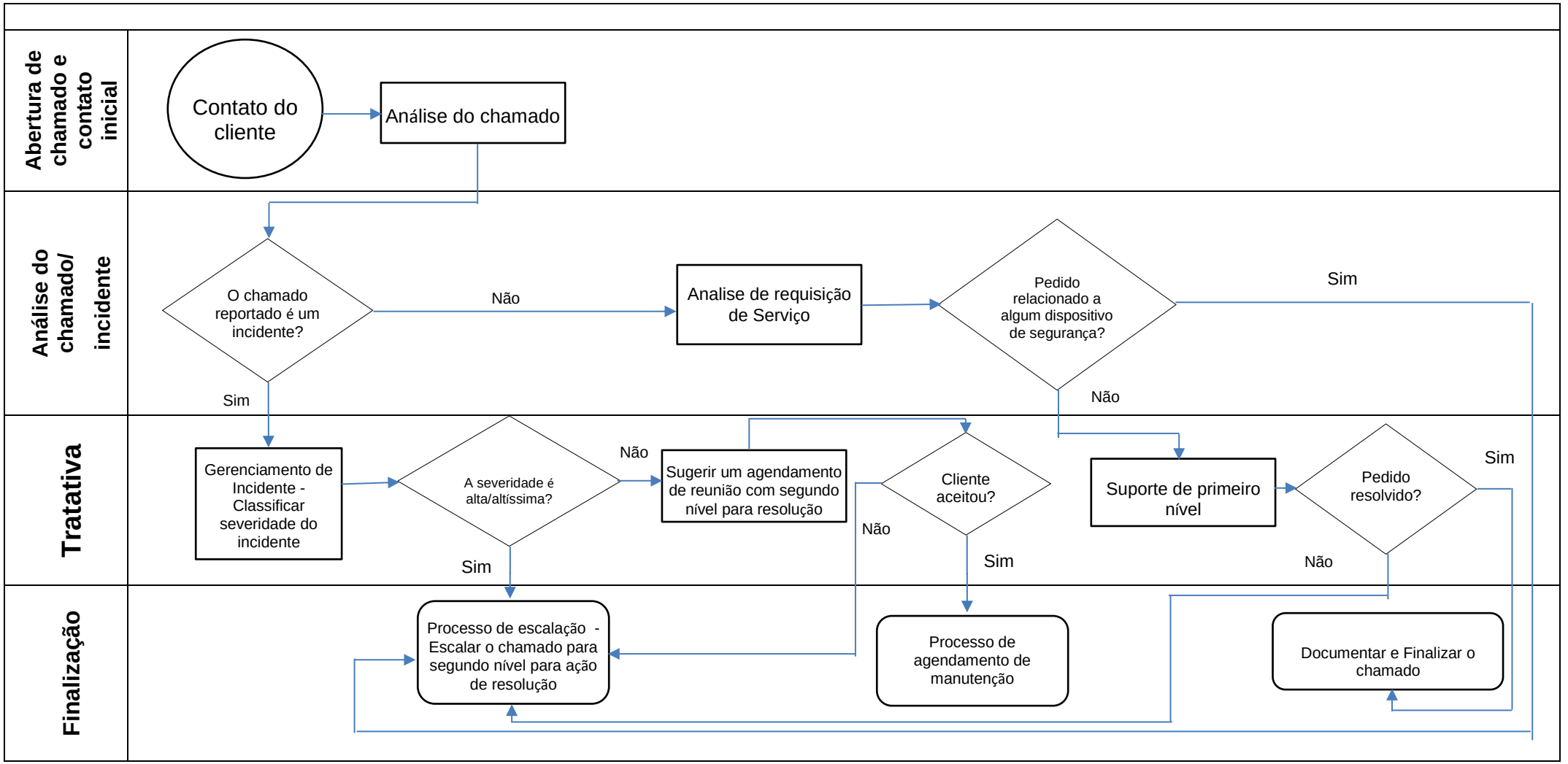
Diante de todas as etapas do ciclo de vida do serviço, desde estratégia de serviço até sua operação, identifica-se que o planejamento é o maior vínculo para o sucesso dos entregáveis, sejam eles serviço ou produto. Planejamento este que conforme orientação e necessidade, é possível aplicar e investigar melhorias a ser aplicadas. Significantemente, podem ser pequenas, mas quando orientadas e mensuradas, tem o poder de mostrar um diferencial competitivo, diminuindo custos, maximizando lucros e possivelmente otimizando processos qualitativos, refletindo assim na satisfação do cliente. Conforme descrito nas etapas, enfatizando o processo de operação de serviço, os processos práticos de execução possibilitam aplicar inovação como forma de ganho, com o objetivo não só de benefício para o negócio, mas sim dos clientes e também do próprio técnico de execução. De grande importância, dentro da operação de serviço, a fase de gerenciamento de incidentes e resolução de requisições podem ser exploradas, através de identificação de tarefas com maior frequência, que podem ser documentados e facilitados para fornecer propriedade aos analistas técnicos de executar os procedimentos de resolução.

2.3 APRESENTAÇÃO DO ATUAL AMBIENTE DE PRESTAÇÃO DE SERVIÇO

Com o entendimento das boas práticas de ITIL, enfatizando o processo de gerenciamento de incidentes, gerenciamento de requisições dentro de operação de serviço e melhoria contínua de serviço, bem como os conceitos técnicos e aprendizagem de segurança da informação, comove-se em aplicar a teoria aprendida dentro de um ambiente de operações de segurança (*SOC*). Baseado neste, a apresentação do ambiente juntamente com a análise dos processos fomenta o objetivo de aplicar melhorias dentro da operação, como um diferencial competitivo operacional e técnico para as partes envolvidas.

Seguindo as boas práticas de ITIL com o modelo de atendimento de prestação de serviço operacional, o centro de operações de segurança estudado tem como objetivo principal gerenciar e fortalecer o ambiente de negócio do cliente através de soluções de prevenção de ataques cibernéticos, gerenciamento de acessos e dispositivos de segurança, análise crítica do negócio, possíveis vulnerabilidades e *pentest*. A prestação de serviço é dividida entre os níveis iniciais de suporte (responsáveis pelo primeiro contato com o cliente) e níveis superiores (responsáveis por tomada de ação, mudanças nos dispositivos de segurança, tratativas de incidente e problemas ou tarefas mais complexas). Enfatizando uma apresentação generalizada porém apontando detalhes relevantes, o modelo operação de atendimento é executado conforme o fluxograma mostrado na figura 2:

Figura 2 – Operação de atendimento atual



Fonte: Autoria Própria

2.3.1 Abertura de chamado e contato inicial

Objetivando documentação e organização, a abertura de chamado é primordial para qualquer tipo de prestação de suporte. O chamado deve ser gerado pelo cliente ou pelo analista (este último utilizando os mecanismos de autenticação) para registro de atividades e detalhes de informações e dados. O cliente pode especificar do que se trata o chamado.

Seguindo esta etapa, o contato inicial com o cliente ocorre com a execução de uma das etapas:

- Contato de telefone: Utilizando o atendimento via telefone do suporte técnico 24x7, o usuário poderá requisitar o suporte passando pelo processo de autenticação por questões de políticas de segurança da informação. Neste processo é requerido a confirmação do login do usuário, número de telefone registrado no sistema e sua frase secreta. O analista poderá prestar suporte somente com a confirmação dessas informações. A abertura do chamado sempre é requerida e, caso o usuário for autenticado, o analista poderá abrir este chamado.

- Chat: Com acesso autorizado ao portal e *website* virtual de segurança, o cliente pode requisitar um pedido ou reportar um incidente através desta opção, aplicando também a mesma política de abertura de chamado para registros.

- *Email*: Este último é opcional para contato inicial do cliente, cujo o mesmo poderá reportar ou requisitar um pedido. Entretanto, por questões de segurança e por mais que hajam mecanismos de prevenção de ameaças ou fraudes por *emails* aplicados, compreende-se que possíveis ataques de *spoofing* via contato de *email* podem ser exercidos. Portanto, como resposta, recomenda-se que o cliente entre em contato com as operações através de contato via telefone, chat ou atualização do chamado no portal virtual.

2.3.2 Análise do chamado/incidente

Conforme o primeiro contato do cliente, aplica-se o processo de análise do chamado. Nesta etapa, é imprescindível que seja feita uma leitura do chamado com o objetivo de entender diretamente do que se trata, quais os impactos, tipo de chamado e sua severidade. É o primeiro passo para início das operações técnicas e esclarecimentos. Feita esta análise, o analista deve entender se a requisição se trata de um incidente ou requisição de serviço.

Enfatizando o processo de requisição de serviço, os motivos de abertura são diversos, quando são introduzidos como pedido de um novo acesso, problemas com acesso a algum recurso, perguntas e questionamentos sobre relatórios e funções dos dispositivos de seguranças, dentre outros. Com maior volume de requisição, os chamados de requisição de mudanças de políticas de acesso de dispositivo de segurança são tratados de acordo com seu SLA (*Service Level Agreement)*, pelo qual o cliente determina quão urgente é o chamado.

As requisições de serviços são classificadas da seguinte forma:

- Problemas com acesso, relatório ou recursos: especificamente para estes casos, o analista inicial terá autonomia para cuidar do chamado. Utilizando procedimentos documentados, o analista dará suporte para o usuário. Em casos de não resolução, o chamado deve ser encaminhado para o segundo nível.

- Requisição de mudanças em *Firewalls/IDS-IPS*: Quando há identificação do chamado como uma requisição de mudança, o chamado é diretamente encaminhado para o segundo nível para processamento. O tempo de processo pode novamente variar de acordo com o SLA estipulado do chamado. Ainda aplicado para este processo, o cliente também tem a opção de agendamento de janela de manutenção.

Em casos de situações de entendimento de incidente, o processo de gerenciamento de incidentes é aplicado seguindo a operação da tratativa.

2.3.3 Tratativa

Após a análise do chamado ou incidente, inicia-se o processo de tratativa, contemplando etapas para classificação de incidentes, tratamento de requisições, tarefas de gerenciamento e triagem de chamados.

2.3.3.1 Gerenciamento de Incidentes

Classificação da severidade do incidente: Para casos determinados como incidente esta é uma etapa crítica do processo. Conforme as boas práticas de ITIL referente à operação de serviço em gerenciamento de incidentes, quando identificado como um incidente do analista técnico deve entender qual o grau de impacto operacional e financeiro do cliente, coletar o máximo de informações e dados. Dentro do processo de classificação de severidade, aplica-se perguntas chaves que podem auxiliar na identificação do impacto ocorrente:

- Pergunta 1: É possível continuar com as operações através de planos de contingência?
- Pergunta 2: Este incidente está causando impacto financeiro?
- Pergunta 3: Você está apto a disponibilizar um administrador de redes e aplicação para auxílio no processo de resolução?

De acordo com as respostas, é possível classificar a severidade do incidente e dar progresso ao suporte. A Tabela 1 mostra a classificação da severidade conforme respostas:

Tabela 1 - Classificação de Severidades

P1	P2	P3	Severidade do Incidente
Não	Sim	Sim	Severidade Altíssima
Não	Não	Sim	Severidade Alta
Não	Não	Não	Severidade Média
Sim	Sim	Sim	Severidade Média
Sim	Sim	Não	Severidade Média
Sim	Não	Não	Severidade Baixa
Sim	Não	Sim	Severidade Baixa
Não	Sim	Não	Severidade Alta

Fonte: Autoria Própria

O tratamento do incidente pode variar de acordo com sua severidade. Ressalta-se que todo e qualquer cliente terá o suporte prestado, independente de sua criticidade, porém, o entendimento do impacto e acuracidade das informações são fatores essenciais para melhor compreensão da situação.

2.3.3.2 Agendamento de janelas de manutenção

Após a identificação da severidade do incidente, em casos de severidade baixa até alta, é sugerida a janela de manutenção com o segundo nível, respeitando a disponibilidade do cliente, demonstrando ao cliente como forma de ganho um recurso dedicado e especialista para resolução do incidente e problema.

2.3.3.3 Suporte de primeiro nível

Seguindo o fluxograma referenciado, chamados não pertencentes a suporte a dispositivos de segurança são tratados pelo suporte inicial. Em geral, estes chamados estão relacionados a problemas com o portal virtual de interação com o cliente, esclarecimento de dúvidas ou relatórios técnicos. Para estes casos, o analista inicial exerce a função de tratamento utilizando documentações de procedimentos existentes, aplicando o processo de escalação para o segundo nível para chamados não solucionados.

2.3.4 Finalização

Contemplando todas as três fases iniciais do modelo de operação de atendimento inicial, a finalização objetiva o encerramento do chamado ou alinhamento e acordo estratégico com o requisitante para dar continuidade ao chamado no futuro, em casos de necessidade de análise profunda do problema ou comodidade das partes envolvidas, determinados pelos processos de finalização.

2.3.4.1 Processo de agendamento de manutenção

Conforme especificado na atividade de tratativa, em casos de severidade baixa até alta, é sugerido ao cliente um agendamento de reunião para resolução no horário desejado. Esta opção é proporcionada para melhor comodidade para o cliente, no qual um recurso exclusivo e especializado fará o tratamento do incidente, envolvendo também previamente outras partes necessárias, como time de redes. Por ser uma opção, o cliente pode ou não aceitar a sugestão. Em caso de aceitação, o analista procede com o agendamento, registrando formalmente o horário em que o cliente deseja, seguindo regras de fuso horário. Todavia, em caso de negação, segue-se o processo de escalação para o segundo nível.

2.3.4.2 Processo de escalação / Incidentes de severidade altíssima

Casos de severidade altíssima, urgência do cliente e não resolução de primeiro nível referente às ferramentas de interações com o cliente são direcionados para o segundo nível. Exclusivamente para incidentes de severidade altíssima, são registradas todas as etapas realizadas e dados coletados para melhor compreender quais atividades já foram executadas pelo analista anterior. A atividade para tratamento de incidentes para severidade altíssima é escalação para o nível superior disponibilizando as informações e dados coletados para tratamento e diagnóstico do incidente. Neste momento, a responsabilidade do analista de primeiro nível é iniciar o processo de documentação das atividades do incidente do início ao fim, tornando-se o gerenciador do incidente, que fará registro dos testes, informações e atividades também trabalhados pelo cliente e toda ação do especialista do segundo nível tratando-se do dispositivo de segurança gerenciado pelas operações. Nenhuma atividade técnica é exercida pelo analista inicial de primeiro nível dentro de todo este processo.

2.3.4.2 Documentar e finalizar o chamado

Em casos nos quais foi possível solucionar a requisição em primeiro plano, é realizada a etapa de documentação, inserindo evidências da tratativa do chamado, como comandos, capturas de tela e toda informação relevante para o cliente e para os analistas em um futuro caso.

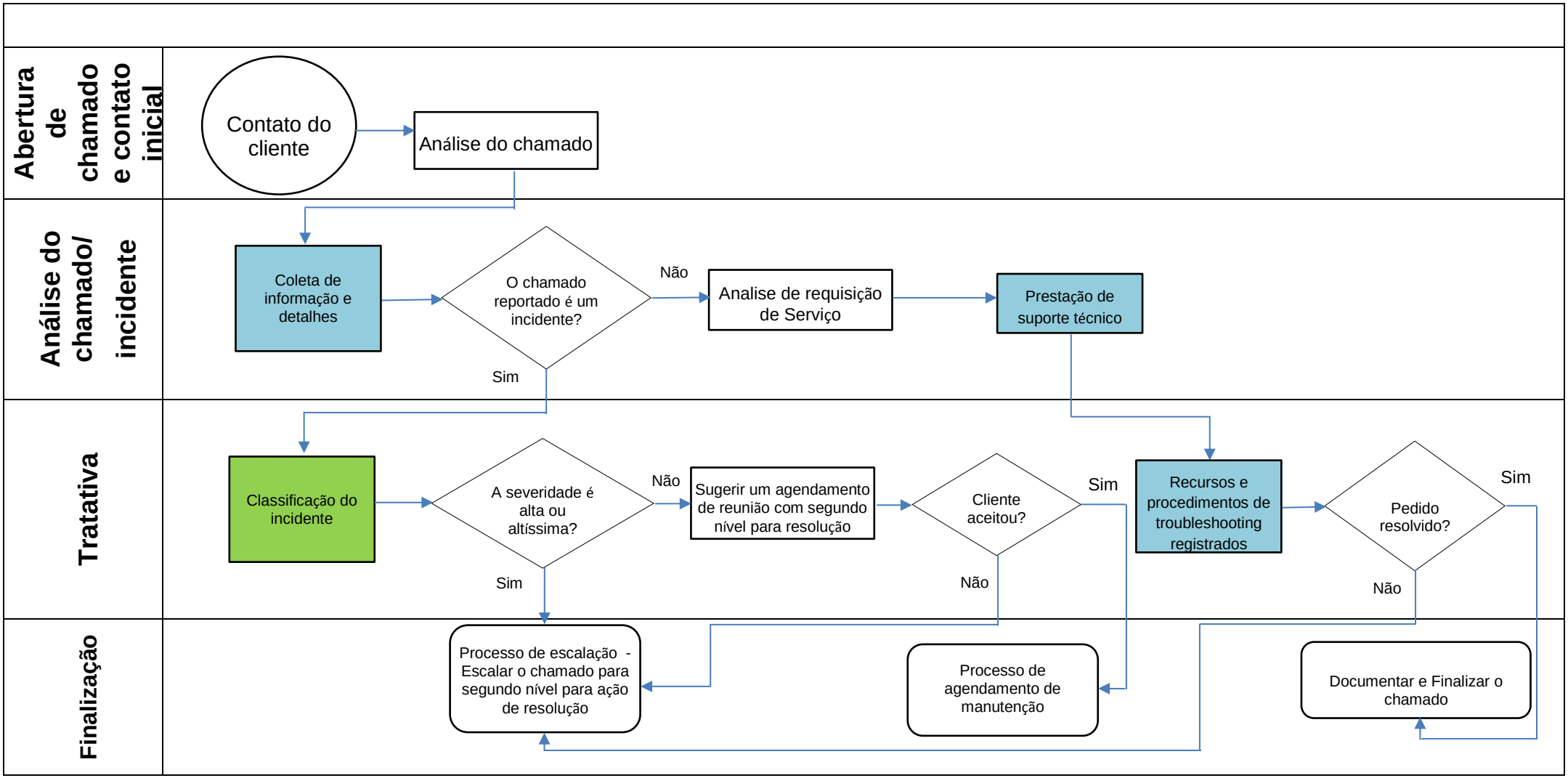
Todas estas atividades e procedimentos em conjunto fomentam o processo de tratamento de gerenciamento de requisições e incidentes dentro das operações de serviço de segurança da informação. Este processo está devidamente envolvido nas atividades diárias dos analistas, tal que dados e informações técnicas são discutidas e a compreensão dos mesmos podem ser valiosos para providenciação de um suporte competitivo e qualitativo.

2.4 PROBLEMATIZAÇÃO

Com o conceito compreendido de inovação e estudo das boas práticas de operação de serviço de ITIL juntamente com o processo de melhoria contínua, podem ser identificados diversos procedimentos com capacidade de melhora. Dentro do processo de gerenciamento de requisições, há falta de aplicação de diagnóstico inicial para possível resolução do chamado ou problema. Existe a oportunidade de explorar tecnicamente alguns procedimentos técnicos que podem resolver requisições, através de registro de chamados anteriores e processos documentados, possibilitando o tempo de resolução e resposta muito menor em relação a casos anteriores. No cenário apresentado referente ao serviço prestado de análise de requisição de serviço ou qualquer atividade relacionada a dispositivos de segurança, nota-se que há rupturas na prestação de serviço técnico limitados para dispositivos de segurança que evidentemente é um dos pontos críticos de prestação de serviço das operações de segurança e do negócio. De uma forma geral, este ponto tem a possibilidade de ser explorado de forma delicada.

Utilizando como princípio o fluxograma de operação de atendimento e buscando a aplicação de inovar o processo e aplicar as boas práticas de melhoria contínua, entende-se a necessidade de reformular este fluxograma apresentando soluções de otimização do processo. Com esta motivação, foi apresentado o novo fluxograma conforme Figura 3:

Figura 3 – Operação de atendimento otimizada



Fonte: Autoria própria

Com base neste novo fluxograma, foram flexibilizadas algumas tarefas com o objetivo de ganho competitivo e valor ao cliente na prestação de atendimento operacional. Estas novas tarefas estão determinadas da seguinte forma:

2.4.1 Coleta de informação e detalhes

O novo procedimento planejado objetiva o entendimento e diagnóstico imediato da requisição ou incidente. Diferente do modelo inicial apresentado, este demonstrará autonomia para o analista de operação inicial e maior maturidade técnica do processo. Além de perguntas para o entendimento do impacto, alguns questionamentos auxiliam no processo de resolução. Utilizando conceitos básicos de segurança da informação e redes, o novo procedimento levantaria os seguintes questionamentos:

- Início da experiência do incidente: Este questionamento é primordial para compreensão de fatores internos ou externos que influenciaram na abertura do chamado. A abertura de mudança de políticas de segurança de um dispositivo solicitadas anteriormente podem ser a causa do incidente. Portanto, estes são questionamentos importantes para compreensão.

- Aplicações, servidores e usuários afetados: A providência de informações de quais usuários estão afetados e/ou servidores afetados colaboram para o diagnóstico. A identificação de quem está acessando (origem) para onde deseja acessar (destino) e sua aplicação (porta) contribui para o analista determinar e analisar nos registros de tráfego onde possivelmente está o problema e, por intermédio de comandos técnicos utilizados nos dispositivos de segurança, determinar se o acesso está ou não permitido.

- Passos de *troubleshoot* já feitos pelo cliente: A compreensão de quais os passos feitos pelo cliente e seu time de redes para diagnóstico cooperam para maior rapidez e agilidade no processo de diagnóstico. Este questionamento é importante para eliminar qualquer tipo de falha de comunicação e de problemas na infraestrutura interna do cliente entre usuário, servidor e redes.

2.4.2 Classificação do incidente

Utilizando a etapa de coleta de informação e detalhes, a classificação do incidente torna-se mais ágil e precisa. Esta etapa concretiza-se exercendo dos mesmos recursos de gerenciamento de incidente e classificação do modelo original, porém de forma mais madura para seguir com continuidade da prestação de serviço.

2.4.3 Prestação de suporte técnico inicial

Com a coleta dessas informações, gera-se um maior entendimento técnico e operacional do chamado ou incidente reportado. Estas informações fomentam as próximas etapas para o diagnóstico do chamado ou incidente, nos quais através de recursos e procedimentos de troubleshooting registrados possibilitam a resolução do incidente logo no primeiro contato feito pelo cliente, evitando escalações e maior carga de trabalho para os níveis superiores de suporte.

2.4.4 Recursos e procedimentos de troubleshooting registrados

Conforme demonstrado no novo plano de processo para gerenciamento de incidentes e especificamente com a resposta dos usuários, servidores e aplicações afetados, o analista inicial de operações dará continuidade ao suporte através do uso de ferramentas de pesquisa no repositório de registros e checagem de política.

- Pesquisa de registros: Para auxílio na busca por registros e identificação de tráfego, todo dispositivo de segurança especificamente *firewalls* gerenciados pelas operações direciona estes registros para os servidores de armazenamento. Estes servidores têm como objetivo serem utilizados para consulta e busca de evidências de tráfego que passam pelo *firewall* do cliente. Conforme argumentado no processo de questionamento de quais os usuários, servidores e aplicações (origem, destino e porta), bem como o início da experiência reportada pelo cliente, é possível fazer pesquisas para comprovar o incidente.

- Checagem de políticas de *firewall*: Através de chamados de incidente bem como chamado de requisições de serviços, o monitoramento e checagem de regras e políticas de *firewall* podem determinar se um acesso está autorizado ou não. Com o entendimento de proposta de gerenciamento dos dispositivos de segurança, as operações gerenciam diversas plataformas de diferentes indústrias. Estas plataformas utilizam seus mecanismos exclusivos de comportamento referente ao tratamento de regras de *firewall*, rotas, VPN, *clusters*, processos entre outros. Conforme essas diferentes funcionalidades, a utilização de material de apoio do próprio fabricante combinados com um documento oficial para busca destes materiais propõe facilidade para o diagnóstico do incidente ou suporte técnico profissional para requisições.

Utilizando esta abordagem, é possível usufruir dos seguintes benefícios:

- Rapidez no atendimento de chamados
- Possível tratativa imediata do problema
- Agregação de atividades similares para os níveis iniciais quando demonstrada autonomia.
- Direcionamento de tarefas mais complexas para os níveis superiores
- Ganho de conhecimento técnico nos níveis iniciais.

2.5 ESTUDO DE CHAMADOS DE PRESTAÇÃO DE SERVIÇO

Com o planejamento de um novo modelo de gerenciamento de incidente e requisições, foi contemplada a necessidade de busca e pesquisa de chamados passados já trabalhados pelos níveis superiores de suporte utilizando o modelo de operação de atendimento inicial para entender sua complexidade e tempo de respostas dos mesmo, cujo o fluxograma e procedimento primário foi aplicado. Com estes princípios, foram extraídos cem chamados trabalhados pelo níveis superiores, utilizando os seguintes critérios:

- Extração de chamados relacionados a gerenciamento de dispositivos de segurança
- Pesquisa inclui plataformas de diferentes fabricantes
- Chamados de incidentes e requisições de serviço
- Chamados relacionados à requisição de mudanças de políticas de segurança e *troubleshooting* VPN foram removidos por questões de política empresarial
- Ainda por questões da política da empresa, chamados de severidade altíssima foram removidos para este estudo.

Com entendimento do tempo de resolução destes chamados, busca-se a mensuração de tempo de resolução destes chamados, para assim realizar o estudo dos resultados comparativos determinando se há ganhos competitivos relacionado a qualidade e satisfação do cliente no atendimento com a implementação do novo modelo de operação.

2.5.1 Classificação dos chamados

Visando a análise, mensuração e comparação clara, os chamados foram classificados em três diferentes tipos de serviço:

- Configuração do dispositivo

Tratam-se de chamados nos quais o requisitante necessita de informações técnicas sobre o dispositivo, exemplificando a versão do *software* instalado, lista de políticas de segurança do dispositivo (quais serviços estão liberados), quais redes atravessam o dispositivo, etc.

- Checagem de tráfego

Quando há questionamentos pelos quais não é possível acessar determinado serviço, servidor ou aplicação, há possibilidade de verificar se o dispositivo está filtrando o tráfego desejado. Nesta atividade, caso o cliente já realizou a tentativa, é possível verificar no dispositivo e servidor de armazenamento de registros de acesso qual foi o comportamento de segurança do dispositivo referente à ação. Além deste, obedecendo a limitação de cada plataforma de segurança, existem recursos para simulação de acesso onde é possível determinar qual será a ação do dispositivo caso o usuário necessite utilizar o recurso (servidor, serviço ou aplicação), através de captura de pacote de rede (*sniffing*) ou rastreamento de pacote (*packet tracer*).

- Questões sobre o dispositivo

Perguntas referente a funcionalidade do dispositivo, que necessita-se saber quais os módulos que estão habilitados (*firewall*, *IDS/IPS*, *VPN*, inspeção *SSL*, etc), uso de recursos do dispositivo (*CPU*, memória, etc) e qualquer outro caso foram classificados como questões sobre o dispositivo.

2.5.2 Análise utilização do modelo inicial de operação de atendimento

Com a classificação destes chamados, questiona-se qual o tempo de resolução de atendimento dos mesmos. De forma estruturada, os cem chamados trabalhados pelo modelo inicial contemplam seus dados divididos da seguinte forma:

- *Ticket*: simples identificação numérica do chamado
- Data de criação: data no qual o chamado foi gerado
- Data de resolução: data no qual o chamado foi solucionado
- Classificação do chamado: diante dos três tipos de classificação, em qual o chamado foi categorizado
- Severidade: qual o grau de severidade classificado para o chamado, independentemente de sua classificação como incidente ou requisição.
- Tempo de resolução (TDR) em horas: tempo que foi necessário para o chamado ser tratado. Este último compõe o tempo total de tratativa, pelos quais diferentes analistas podem ter exercido atividades de trabalho no chamado.

Com a realização e estruturação e entendimento da informação, a tabela 2 demonstra os resultados de coleta de dados de utilização do modelo inicial (chamados trabalhados pelos níveis superiores):

Tabela 2 – Coleta de chamados do modelo de operação de atendimento inicial

Ticket	Data de criação	Data de resolução	Classificação do chamado	Severidade	TDR (h)
962583	2/1/19 12:29	2/1/19 16:18	Checagem de tráfego	Baixa	3.8
963095	2/1/19 21:34	2/1/19 22:52	Checagem de tráfego	Média	1.3
964954	3/1/19 14:02	3/1/19 16:47	Configuração do dispositivo	Baixa	2.8
965565	3/1/19 19:09	4/1/19 16:23	Checagem de tráfego	Média	21.2
966235	4/1/19 5:37	4/1/19 9:53	Checagem de tráfego	Média	4.3
966850	4/1/19 17:51	8/1/19 14:45	Configuração do dispositivo	Média	20.9
966975	4/1/19 19:49	4/1/19 20:46	Checagem de tráfego	Média	0.9
967206	5/1/19 2:49	5/1/19 5:51	Checagem de tráfego	Média	3.0
969618	7/1/19 10:03	8/1/19 14:27	Configuração do dispositivo	Baixa	12.4
969957	7/1/19 13:58	7/1/19 20:07	Configuração do dispositivo	Baixa	6.1
969997	7/1/19 15:00	8/1/19 11:48	Questões sobre o dispositivo	Média	20.8
970337	7/1/19 18:35	7/1/19 21:02	Checagem de tráfego	Média	2.4
971463	8/1/19 11:55	8/1/19 12:20	Checagem de tráfego	Média	0.4
971473	8/1/19 12:28	8/1/19 14:22	Checagem de tráfego	Baixa	1.9
972090	8/1/19 18:08	10/1/19 1:14	Configuração do dispositivo	Média	7.1
972219	8/1/19 18:42	8/1/19 19:11	Configuração do dispositivo	Média	0.5
973281	9/1/19 2:19	9/1/19 6:18	Checagem de tráfego	Média	4.0
973370	9/1/19 4:35	9/1/19 7:23	Checagem de tráfego	Média	2.8
973857	9/1/19 11:04	9/1/19 13:02	Configuração do dispositivo	Média	2.0
973865	9/1/19 11:26	9/1/19 12:40	Configuração do dispositivo	Média	1.2
974134	9/1/19 13:36	9/1/19 20:40	Checagem de tráfego	Média	7.1
975263	10/1/19 2:38	10/1/19 13:38	Checagem de tráfego	Média	11.0
975316	10/1/19 4:56	10/1/19 14:04	Checagem de tráfego	Média	9.1
976047	10/1/19 13:18	11/1/19 2:34	Configuração do dispositivo	Média	13.3
977682	11/1/19 13:38	11/1/19 18:19	Configuração do dispositivo	Média	4.7
981090	14/1/19 14:00	15/1/19 0:28	Configuração do dispositivo	Média	10.5
981230	14/1/19 17:10	15/1/19 2:57	Configuração do dispositivo	Média	9.8
981581	14/1/19 19:34	15/1/19 0:59	Configuração do dispositivo	Média	5.4
982167	15/1/19 4:07	15/1/19 10:03	Checagem de tráfego	Alta	5.9
982901	15/1/19 12:52	15/1/19 14:52	Checagem de tráfego	Média	2.0
983247	15/1/19 14:20	15/1/19 17:10	Checagem de tráfego	Média	2.8
984698	16/1/19 6:25	17/1/19 1:44	Questões sobre o dispositivo	Média	19.3
984798	16/1/19 7:03	16/1/19 8:19	Checagem de tráfego	Alta	1.3
986414	17/1/19 6:58	17/1/19 8:43	Checagem de tráfego	Baixa	1.7
987499	17/1/19 18:17	18/1/19 19:04	Checagem de tráfego	Baixa	24.8
988367	18/1/19 6:30	18/1/19 7:22	Configuração do dispositivo	Média	0.9
988912	18/1/19 16:45	19/1/19 19:41	Configuração do dispositivo	Alta	21.9
989238	18/1/19 17:27	22/1/19 7:00	Checagem de tráfego	Média	13.5

Ticket	Data de criação	Data de resolução	Classificação do chamado	Severidade	TDR (h)
989363	18/1/19 18:34	18/1/19 19:45	Checagem de tráfego	Média	1.2
989315	18/1/19 19:51	18/1/19 23:28	Configuração do dispositivo	Média	3.6
990892	19/1/19 21:06	20/1/19 2:59	Checagem de tráfego	Alta	5.9
992757	21/1/19 3:04	21/1/19 9:07	Configuração do dispositivo	Baixa	6.0
993680	21/1/19 16:44	22/1/19 19:41	Configuração do dispositivo	Baixa	3.0
994153	21/1/19 17:25	21/1/19 18:55	Configuração do dispositivo	Média	1.5
994335	21/1/19 18:13	22/1/19 7:51	Checagem de tráfego	Média	13.6
994686	21/1/19 21:02	22/1/19 11:43	Checagem de tráfego	Baixa	14.7
994859	21/1/19 23:39	22/1/19 14:04	Configuração do dispositivo	Alta	14.4
995711	22/1/19 12:15	23/1/19 18:00	Configuração do dispositivo	Média	4.8
996026	22/1/19 17:19	22/1/19 22:49	Checagem de tráfego	Baixa	5.5
997269	23/1/19 0:06	23/1/19 1:27	Questões sobre o dispositivo	Média	1.4
997977	23/1/19 12:25	23/1/19 15:23	Configuração do dispositivo	Média	3.0
998434	23/1/19 16:17	24/1/19 1:37	Configuração do dispositivo	Baixa	9.3
998274	23/1/19 17:56	23/1/19 20:02	Questões sobre o dispositivo	Baixa	2.1
2003	25/1/19 13:56	25/1/19 18:07	Checagem de tráfego	Média	4.2
6922	28/1/19 12:35	28/1/19 23:35	Checagem de tráfego	Baixa	11.0
7342	28/1/19 14:16	29/1/19 4:44	Questões sobre o dispositivo	Média	14.5
7551	28/1/19 16:17	28/1/19 20:27	Questões sobre o dispositivo	Média	4.2
7921	28/1/19 21:10	29/1/19 0:07	Configuração do dispositivo	Média	3.0
9792	29/1/19 16:24	29/1/19 18:10	Checagem de tráfego	Média	1.8
11392	29/1/19 22:18	30/1/19 2:12	Configuração do dispositivo	Média	3.9
12192	30/1/19 9:51	31/1/19 7:01	Checagem de tráfego	Baixa	21.2
12662	30/1/19 16:12	30/1/19 18:09	Configuração do dispositivo	Baixa	2.0
12810	30/1/19 19:59	30/1/19 23:59	Configuração do dispositivo	Baixa	4.0
13016	30/1/19 21:35	31/1/19 11:21	Configuração do dispositivo	Baixa	13.8
13214	31/1/19 1:46	31/1/19 3:04	Configuração do dispositivo	Média	1.3
14674	31/1/19 18:10	31/1/19 21:41	Configuração do dispositivo	Média	3.5
483318	2/4/18 14:52	2/4/18 17:40	Questões sobre o dispositivo	Média	2.8
483418	2/4/18 16:01	4/4/18 19:46	Questões sobre o dispositivo	Média	3.8
483642	2/4/18 17:44	3/4/18 22:56	Configuração do dispositivo	Média	6.2
486159	4/4/18 1:27	4/4/18 18:57	Checagem de tráfego	Média	17.5
486331	4/4/18 4:37	4/4/18 13:46	Checagem de tráfego	Média	9.2
487155	4/4/18 15:39	4/4/18 18:45	Checagem de tráfego	Média	3.1
489302	5/4/18 15:20	5/4/18 17:31	Checagem de tráfego	Média	2.2
490844	6/4/18 15:11	8/4/18 1:15	Configuração do dispositivo	Média	10.1
490877	6/4/18 15:21	6/4/18 22:30	Questões sobre o dispositivo	Média	7.2
491135	6/4/18 18:42	6/4/18 20:25	Questões sobre o dispositivo	Média	1.7
491594	7/4/18 2:57	9/4/18 11:04	Configuração do dispositivo	Média	8.1
493936	9/4/18 7:28	9/4/18 20:05	Questões sobre o dispositivo	Média	12.6
494185	9/4/18 10:46	9/4/18 14:58	Configuração do dispositivo	Média	4.2
494953	9/4/18 19:20	10/4/18 18:28	Checagem de tráfego	Média	23.1

Ticket	Data de criação	Data de resolução	Classificação do chamado	Severidade	TDR (h)
495702	10/4/18 3:55	10/4/18 13:18	Questões sobre o dispositivo	Média	9.4
498837	11/4/18 11:45	11/4/18 14:28	Questões sobre o dispositivo	Média	2.7
499277	11/4/18 15:40	12/4/18 0:44	Questões sobre o dispositivo	Média	9.1
499329	11/4/18 16:05	11/4/18 16:34	Questões sobre o dispositivo	Média	0.5
501585	12/4/18 15:26	14/4/18 18:17	Configuração do dispositivo	Média	7.8
502545	13/4/18 6:38	13/4/18 20:08	Questões sobre o dispositivo	Média	13.5
502746	13/4/18 10:02	13/4/18 12:06	Configuração do dispositivo	Média	2.1
502863	13/4/18 11:36	14/4/18 3:40	Checagem de tráfego	Média	16.1
502897	13/4/18 12:06	14/4/18 2:04	Checagem de tráfego	Média	14.0
504077	14/4/18 6:14	14/4/18 21:33	Configuração do dispositivo	Média	15.3
944087	18/12/18 20:30	18/12/18 21:22	Checagem de tráfego	Média	0.9
945085	19/12/18 14:53	19/12/18 18:34	Configuração do dispositivo	Média	3.7
945402	19/12/18 15:43	19/12/18 18:26	Questões sobre o dispositivo	Média	2.7
945504	19/12/18 18:36	19/12/18 19:07	Checagem de tráfego	Média	0.5
945849	19/12/18 19:55	20/12/18 8:35	Configuração do dispositivo	Média	12.7
945850	19/12/18 19:55	20/12/18 5:34	Configuração do dispositivo	Média	9.6
936990	14/12/18 0:00	14/12/18 17:01	Questões sobre o dispositivo	Média	17.0
938155	14/12/18 16:36	14/12/18 19:03	Questões sobre o dispositivo	Média	2.5
938053	14/12/18 16:41	14/12/18 23:36	Configuração do dispositivo	Média	6.9
938216	14/12/18 17:37	14/12/18 23:58	Checagem de tráfego	Média	6.3

Fonte: Autoria Própria

Resultados e análise do modelo inicial

Diante dos dados estruturados apresentados na tabela, para melhor compreensão e transformação dos mesmos em informação comparativa, realiza-se a seguinte conclusão:

Número de chamados para cada classificação:

- Quarenta e um chamados para **Configuração do dispositivo**
- Quarenta chamados para **Checagem de tráfego**
- Dezenove chamados para **Questões sobre o dispositivo**

Análise do tempo de resolução:

Revisando os dados apresentados de tempo de resolução em horas, conclui-se os seguintes resultados para os cálculos de média, moda e mediana:

- O tempo de resolução médio dos chamados foi de 7 horas e 18 minutos.
- O tempo de resolução com a realização do cálculo de mediana foi de 4 horas e 48 minutos.
- O tempo de resolução com a realização do cálculo de moda foi de 2 horas e 48 minutos.

Conforme a análise explorada do modelo inicial de operação de atendimento e dos chamados coletados, há uma grande divergência e variação de tempo de resolução de cada chamado. Com o objetivo do estudo técnico destes chamados, a análise e apresentação dos resultados utilizando o modelo de operação de atendimento otimizado é relevante para realizar o grau comparativo e estudar possíveis ganhos com sua utilização.

2.5.3 Utilização do modelo de operação de atendimento otimizado

Visando este comportamento e entusiasmo, foram coletados também cem chamados utilizando o novo modelo de operação de atendimento. Seguindo paralelamente os mesmos critérios originais do modelo inicial, para exercício de comparação justo e realista. Estes chamados foram trabalhados somente pelo nível técnico inicial, utilizando as melhorias de processo referente a autonomia de execução de processos de atendimento com a determinação de explorar qual foi o possível ganho de tempo de resolução dos chamados. A tabela 3 mostra os resultados:

Tabela 3 – Coleta de chamados do modelo de operação de atendimento otimizado

Ticket	Data de criação	Data de resolução	Classificação do chamado	Severidade	TDR
962883	2/1/19 16:56	2/1/19 19:50	Checagem de tráfego	Baixa	2.9
965178	3/1/19 16:55	3/1/19 18:22	Checagem de tráfego	Média	1.5
965819	4/1/19 0:27	4/1/19 1:45	Configuração do dispositivo	Baixa	1.3
977440	11/1/19 4:23	11/1/19 6:22	Checagem de tráfego	Média	2.0
977849	11/1/19 11:52	11/1/19 12:12	Checagem de tráfego	Média	0.3
981052	14/1/19 12:34	14/1/19 13:48	Configuração do dispositivo	Baixa	1.2
983376	15/1/19 16:34	15/1/19 18:43	Checagem de tráfego	Média	2.2
983481	15/1/19 17:27	15/1/19 18:23	Checagem de tráfego	Média	0.9
985238	16/1/19 13:50	16/1/19 16:44	Configuração do dispositivo	Média	2.9
985259	16/1/19 14:17	16/1/19 17:29	Configuração do dispositivo	Baixa	3.2
987314	17/1/19 18:01	17/1/19 19:00	Questões sobre o dispositivo	Média	1.0
987683	17/1/19 21:15	18/1/19 21:06	Checagem de tráfego	Média	23.9
994663	21/1/19 20:33	21/1/19 21:03	Checagem de tráfego	Média	0.5
996055	22/1/19 15:20	22/1/19 15:55	Checagem de tráfego	Média	0.6
435	24/1/19 16:25	24/1/19 17:49	Configuração do dispositivo	Média	1.4
652	24/1/19 19:13	24/1/19 19:54	Configuração do dispositivo	Média	0.7
6169	27/1/19 17:35	27/1/19 18:20	Checagem de tráfego	Média	0.8
16555	1/2/19 19:53	1/2/19 20:06	Checagem de tráfego	Média	0.2
16821	1/2/19 22:07	2/2/19 0:36	Configuração do dispositivo	Média	2.5
19318	4/2/19 10:41	4/2/19 13:36	Configuração do dispositivo	Média	2.9
21497	4/2/19 19:39	4/2/19 21:01	Checagem de tráfego	Média	1.4
23469	5/2/19 20:00	5/2/19 22:02	Checagem de tráfego	Média	2.0
24791	6/2/19 15:25	6/2/19 16:55	Checagem de tráfego	Média	1.5
25087	6/2/19 20:10	6/2/19 21:14	Configuração do dispositivo	Alta	1.1
25273	7/2/19 0:26	7/2/19 0:36	Configuração do dispositivo	Média	0.2
28318	8/2/19 20:16	8/2/19 20:39	Configuração do dispositivo	Alta	0.4
35632	11/2/19 16:37	11/2/19 19:21	Configuração do dispositivo	Baixa	2.7
37545	12/2/19 19:11	12/2/19 20:09	Configuração do dispositivo	Média	1.0
40592	14/2/19 0:19	14/2/19 5:40	Checagem de tráfego	Alta	5.3
41297	14/2/19 13:11	14/2/19 17:37	Checagem de tráfego	Média	4.4
44029	16/2/19 9:28	16/2/19 13:10	Checagem de tráfego	Média	3.7
47367	18/2/19 23:01	19/2/19 0:11	Questões sobre o dispositivo	Média	1.2
48149	19/2/19 12:24	19/2/19 13:08	Checagem de tráfego	Alta	0.7
51000	20/2/19 12:52	20/2/19 18:06	Checagem de tráfego	Baixa	5.2
53805	21/2/19 19:26	21/2/19 20:16	Checagem de tráfego	Baixa	0.8
54123	22/2/19 0:29	22/2/19 0:50	Configuração do dispositivo	Média	0.3
54823	22/2/19 14:12	22/2/19 20:59	Configuração do dispositivo	Média	6.8
59114	25/2/19 20:07	25/2/19 20:52	Checagem de tráfego	Baixa	0.8
60785	26/2/19 21:50	26/2/19 22:14	Checagem de tráfego	Alta	0.4
62199	27/2/19 14:38	27/2/19 18:40	Configuração do dispositivo	Média	4.0
62204	27/2/19 14:49	27/2/19 21:44	Checagem de tráfego	Baixa	6.9

Ticket	Data de criação	Data de resolução	Classificação do chamado	Severidade	TDR
62224	27/2/19 15:26	27/2/19 19:42	Configuração do dispositivo	Média	4.3
62436	27/2/19 15:50	27/2/19 19:59	Configuração do dispositivo	Média	4.2
64680	28/2/19 18:53	1/3/19 0:49	Configuração do dispositivo	Baixa	5.9
65981	1/3/19 6:51	1/3/19 7:40	Checagem de tráfego	Baixa	0.8
69149	4/3/19 4:11	4/3/19 4:32	Checagem de tráfego	Média	0.3
73409	7/3/19 0:20	7/3/19 0:33	Configuração do dispositivo	Baixa	0.2
74417	7/3/19 11:03	7/3/19 14:04	Configuração do dispositivo	Média	3.0
74782	7/3/19 14:57	7/3/19 18:34	Checagem de tráfego	Média	3.6
74654	7/3/19 15:01	7/3/19 17:45	Questões sobre o dispositivo	Média	2.7
76080	8/3/19 13:24	8/3/19 21:19	Configuração do dispositivo	Média	7.9
76745	8/3/19 18:50	8/3/19 22:13	Configuração do dispositivo	Média	3.4
80291	11/3/19 12:23	11/3/19 15:41	Questões sobre o dispositivo	Baixa	3.3
80568	11/3/19 12:44	11/3/19 18:16	Checagem de tráfego	Baixa	5.5
81629	11/3/19 21:29	11/3/19 22:55	Checagem de tráfego	Baixa	1.4
83148	12/3/19 19:23	12/3/19 20:52	Questões sobre o dispositivo	Baixa	1.5
84472	13/3/19 12:59	13/3/19 19:47	Questões sobre o dispositivo	Média	6.8
85140	13/3/19 17:57	13/3/19 22:02	Configuração do dispositivo	Média	4.1
93600	18/3/19 22:46	19/3/19 6:37	Checagem de tráfego	Média	7.8
93961	19/3/19 4:00	19/3/19 4:39	Configuração do dispositivo	Média	0.6
101644	22/3/19 20:13	22/3/19 21:10	Checagem de tráfego	Média	1.0
101645	22/3/19 20:14	22/3/19 21:04	Configuração do dispositivo	Média	0.8
108863	27/3/19 0:53	27/3/19 2:28	Configuração do dispositivo	Média	1.6
110396	27/3/19 23:08	28/3/19 0:22	Configuração do dispositivo	Média	1.2
111351	28/3/19 13:13	28/3/19 18:47	Configuração do dispositivo	Média	5.6
111790	28/3/19 18:20	28/3/19 19:44	Configuração do dispositivo	Média	1.4
119467	1/4/19 11:57	1/4/19 19:38	Questões sobre o dispositivo	Média	7.7
121992	2/4/19 23:27	3/4/19 2:28	Questões sobre o dispositivo	Média	3.0
121993	2/4/19 23:27	3/4/19 1:43	Configuração do dispositivo	Média	2.3
122627	3/4/19 10:10	3/4/19 18:35	Checagem de tráfego	Média	8.4
122892	3/4/19 13:18	3/4/19 19:02	Checagem de tráfego	Média	5.7
131298	9/4/19 0:41	9/4/19 1:48	Checagem de tráfego	Média	1.1
131423	9/4/19 3:15	9/4/19 4:49	Checagem de tráfego	Média	1.6
136792	11/4/19 14:38	11/4/19 18:53	Configuração do dispositivo	Média	4.2
139001	12/4/19 12:32	12/4/19 14:51	Questões sobre o dispositivo	Média	2.3
140990	13/4/19 14:23	13/4/19 16:31	Questões sobre o dispositivo	Média	2.1
140991	13/4/19 14:23	13/4/19 17:00	Configuração do dispositivo	Média	2.6
142665	14/4/19 19:26	14/4/19 20:13	Questões sobre o dispositivo	Média	0.8
143123	15/4/19 6:14	15/4/19 8:11	Configuração do dispositivo	Média	1.9
144543	15/4/19 21:05	15/4/19 22:53	Checagem de tráfego	Média	1.8
144645	16/4/19 0:03	16/4/19 2:09	Questões sobre o dispositivo	Média	2.1
154320	22/4/19 13:54	22/4/19 17:54	Questões sobre o dispositivo	Média	4.0
158948	23/4/19 18:35	23/4/19 20:10	Questões sobre o dispositivo	Média	1.6

Ticket	Data de criação	Data de resolução	Classificação do chamado	Severidade	TDR
159779	23/4/19 23:30	23/4/19 23:47	Questões sobre o dispositivo	Média	0.3
164734	26/4/19 15:00	26/4/19 17:00	Configuração do dispositivo	Média	2.0
167562	29/4/19 8:36	29/4/19 10:59	Questões sobre o dispositivo	Média	2.4
169033	29/4/19 17:40	29/4/19 19:25	Configuração do dispositivo	Média	1.8
169052	29/4/19 18:45	29/4/19 19:21	Checagem de tráfego	Média	0.6
171046	1/5/19 0:31	1/5/19 0:39	Checagem de tráfego	Média	0.1
172295	1/5/19 20:24	1/5/19 22:05	Configuração do dispositivo	Média	1.7
172442	1/5/19 21:35	1/5/19 22:53	Checagem de tráfego	Média	1.3
175657	3/5/19 19:28	4/5/19 0:24	Configuração do dispositivo	Média	4.9
195666	15/5/19 16:53	15/5/19 18:07	Questões sobre o dispositivo	Média	1.2
197238	16/5/19 14:31	16/5/19 17:05	Checagem de tráfego	Média	2.6
196418	16/5/19 14:38	16/5/19 17:26	Configuração do dispositivo	Média	2.8
197349	16/5/19 14:57	16/5/19 17:37	Configuração do dispositivo	Média	2.7
204320	20/5/19 20:40	20/5/19 21:49	Questões sobre o dispositivo	Média	1.2
221494	28/5/19 14:55	28/5/19 18:14	Questões sobre o dispositivo	Média	3.3
221574	28/5/19 16:11	28/5/19 17:57	Configuração do dispositivo	Média	1.8
223608	29/5/19 23:06	30/5/19 0:39	Checagem de tráfego	Média	1.6

Fonte: Autoria Própria

Resultados e análise do novo modelo:

Número de chamados para cada classificação:

- Quarenta e um chamados para **Configuração do dispositivo**
- Quarenta chamados para **Checagem de tráfego**
- Dezenove chamados para **Questões sobre o dispositivo**

Análise do tempo de resolução:

Revisando os dados apresentados de tempo de resolução em horas, conclui-se os seguintes resultados para os cálculos de média, moda e mediana:

- O tempo de resolução médio dos chamados foi de 2 horas e 42 minutos.
- O tempo de resolução com a realização do cálculo de mediana foi de 1 horas e 54 minutos.
- O tempo de resolução com a realização do cálculo de moda foi de 48 minutos.

3 RESULTADOS

Estudo comparativo dos modelos

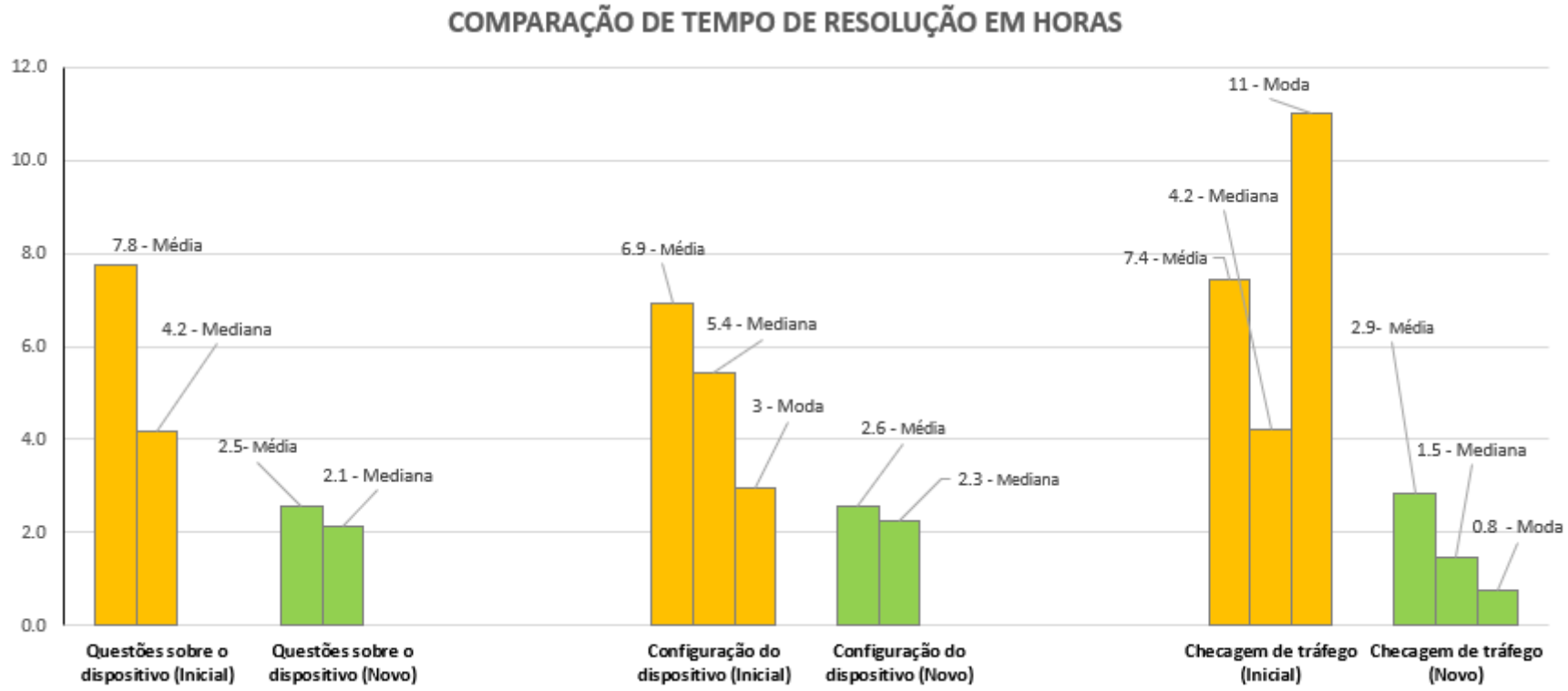
Em concordância com os dados e resultados apresentados dos modelos, visa-se entender quais foram os ganhos operacionais do processo e consequentemente da operação de negócio. A tabela 4 e o gráfico conforme figura 4 demonstra o grau comparativo dos processos especificando os diferentes tipos de classificação, utilizando os resultados estatísticos de média, mediana e moda:

Tabela 4 – Comparação dos modelos: classificação dos chamados

Classificação	Modelo inicial (Média)	Modelo inicial (Mediana)	Modelo inicial (Moda)
Questões sobre o dispositivo	7.8	4.2	#N/A
Configuração do dispositivo	6.9	5.4	3
Checagem de tráfego	7.4	4.2	11

Classificação	Novo modelo (Média)	Novo modelo (Mediana)	Novo modelo (Moda)
Questões sobre o dispositivo	2.5	2.1	#N/A
Configuração do dispositivo	2.6	2.3	#N/A
Checagem de tráfego	2.9	1.5	0.8

Figura 4: Gráfico comparativo de tempo de resolução do modelo inicial e modelo otimizado.



Fonte: Autoria Própria

Com a estruturação das informações, bem como a análise da tabela de resultados e a informação que o gráfico propõe referente aos casos estudados, é possível entender que houve diminuição consideravelmente relevante perante a comparação do modelo inicial e modelo novo apresentado como forma de inovação. A partir deste, conseguimos entender que houve otimização no tempo de resolução para todas as classificações de chamados, sendo estes resultados formados da seguinte forma em primeiro plano:

- Para chamados referente às questões sobre o dispositivo, houve uma diminuição de tempo de resolução de 68% para o cálculo geral de média e 50% para mediana

- Chamados classificados como configuração de dispositivo, a redução foi de 62,3% para média e 57,4% para mediana.

- Nas requisições listadas como checagem de tráfego, foi possível observar a melhora no atendimento com resultados demonstrados em 60,8% de diminuição pertencente ao cálculo de média e 64,3% para mediana.

Entendendo a análise trabalhada, compreende-se que a abordagem e aplicação do modelo de operação de atendimento otimizado apresentou melhora significativa no atendimento e resolução de chamados de serviços de segurança da informação, independentemente da classificação dos chamados. Classificação esta que foi originalizada pelo conhecimento adquirido de inovação e aplicação de melhoria contínua em operações, que mostrou ser efetivo através da estruturação dos processos de forma que seja possível a mensuração e análise crítica do serviço, para assim demonstrar maior maturidade e alinhamento com as boas práticas de ITIL.

4 CONSIDERAÇÕES FINAIS

Com a análise do processo de atendimento ao cliente na prestação de serviços de segurança e suas etapas de operação, o uso e conceito de inovação dentro do ambiente de centro de operações de segurança foi primordial para exploração de novas oportunidades, enfatizando como diferencial competitivo o uso das melhoras práticas de ITIL que é conhecida por diversos nichos de tecnologia da informação.

Foi observado e visualizado fortemente o uso do ciclo de vida do serviço e suas fases no uso das melhoras práticas de ITIL com destaque nos processos de estratégia de serviço, operação e melhoria contínua, objetivando um atendimento qualitativo responsável em satisfazer o negócio do cliente com maturidade. O uso efetivo destes recursos demonstrou a forte influência para estudo e geração do relatório técnico, realizando questionamentos de quais etapas e procedimentos poderiam ser melhorados fomentando o uso de processos de melhoria contínua e sua influência através das melhores práticas. Isto consequentemente gerou a capacitação para entender e problematizar o modelo de atendimento operacional inicial sendo utilizado, com o consentimento e olhar crítico dos processos de capacidade de otimização. Através das informações dos processos extraídos, foi possível mapear cada etapa e seu procedimento para então a identificação de possíveis melhorias a serem aplicadas. Utilizando a extração desta informação, foi mapeado quais etapas haviam capacidade de melhora e aplicação de um procedimento mais maduro e inteligente. Procedimento este que incentivou a criação de um novo fluxograma com objetivo de alinhamento de processo e ganho competitivo para todas as partes envolvidas, sejam elas clientes internos ou externos.

A aplicação do novo processo de operação de atendimento influenciou diretamente nos resultados operacionais de atendimento dos chamados. A partir da análise de resultados bem como a comparação do modelo anterior com o novo modelo, foi possível obter uma grande e relevante redução no tempo de atendimento dos chamados e prestação de serviço para todas as classificações estudadas, demonstrando maturidade no processo de atendimento após a aplicação de melhorias no atendimento. Coincidente do ganho da prestação do serviço, conclui-se que além do tempo de resposta obtiveram-se otimizações em relação a qualidade e satisfação do cliente, uma vez que suas requisições e chamados são entregados com mais agilidade e eficiência sem perder sua qualidade. Além deste, a otimização do processo impulsiona o desenvolvimento técnico do analista de primeiro nível, criando oportunidades de carreira técnica para desenvolvimento e futuramente alocação para níveis superiores. Por fim, ocorre de forma a distribuição de tarefas com maior

complexidade para os níveis superiores, com capacidade de aplicar análises e tratativa de problemas mais críticos

Finalmente, com base no relatório técnico desenvolvido e todo o material teórico trabalhado e estudado, conseguiu-se com sucesso entender a importância do uso das melhoras práticas de ITIL em processos específicos de prestação de serviço de segurança da informação, no qual é possível aplicar mudanças e melhorias sem custos adicionais, que fortalecem diretamente a satisfação do cliente de forma positiva e criam oportunidades internas de desenvolvimento, valores e competência para concretizar a continuidade do negócio de forma inteligente.

REFERÊNCIAS BIBLIOGRÁFICAS:

ADAIR, J. **Leadership for Innovation**: How to Organize Team Creativity and Harvest Ideas. Disponível em < https://www.safaribooksonline.com/library/view/leadership-for-innovation/9780749454791/>. Acesso em: 25 maio 2019. 12h43.

AGUTTER, C. **ITIL Lifecycle Essentials**. Disponível em < https://www.safaribooksonline.com/library/view/itil-lifecycle-essentials/9781849284196/>. Acesso em: 25 maio 2019. 15h43.

DRUCKER, P. F. **Inovação e Espírito Empreendedor**: Prática e Princípios. Tradução de: Carlos Malferrari. São Paulo: Cengage Learning. 2014.

GLOBAL KNOWLEDGE. **ITIL Foundation.** Cary, NC. USA. Global Knowledge Training LLC. 2016.

MAGALHÃES, I. L., PINHEIRO, W., V. **Gerenciamento de Serviços de TI na Prática**: Uma abordagem com base na ITIL. Rio de Janeiro: Novatec. 2007.

MILLS, K., HOVE, V. S. **It's All About Relationships**: What ITIL Does Not Tell You. Disponível em < https://www.safaribooksonline.com/library/view/its-all-about/9781849284998/> Acesso em: 25 maio 2019. 17h43.

MELO, J., L., OLIVEIRA, A., V., ALMEIDA, B., L. **Guia Preparatório para Certificação ITIL Foundation.** Exame EX0-001. Rio de Janeiro. Nova Terra. 2017.