PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS E DE TECNOLOGIAS

PABLO GULIAS RUFINO DE FREITAS

SEGURANÇA DA INFORMAÇÃO E QoS NA GESTÃO DE REDES DE TELECOMUNICAÇÕES EM CONFORMIDADE COM ITIL

CAMPINAS
2017

PABLO GULIAS RUFINO DE FREITAS

SEGURANÇA DA INFORMAÇÃO E QoS NA GESTÃO DE REDES DE TELECOMUNICAÇÕES EM CONFORMIDADE COM ITIL

Dissertação apresentada como requisito parcial para a obtenção do título de Mestre em Gestão de Redes de Telecomunicações, do Centro de Ciências Exatas, Ambientais e Tecnologias, da Pontifícia Universidade Católica de Campinas.

Orientador: Professor Dr. Eric Alberto de Mello Fagotto

PUC-CAMPINAS
2017

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS
CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS E DE TECNOLOGIA
FACULDADE DE ENGENHARIA ELÉTRICA

Autor: GULIAS RUFINO DE FREITAS, Pablo
Título: Segurança da informação e QoS na gestão de redes de telecomunicações em conformidade com ITIL

Dissertação de Mestrado em Gestão de Redes de Telecomunicações

BANCA EXAMINADORA

Presidente e Orientador Prof. Dr. Eric Alberto de Mello Fagotto – Pontifícia Universidade Católica de Campinas

_____

1º Examinador Prof. Dr. Edson Luiz Ursini – Universidade Estadual de Campinas

_____

2º Examinador Prof. Dr. David Bianchini – Pontifícia Universidade Católica de Campinas

_____

Campinas, 02 de maio de 2017.

Aos meus pais, Wilma e Severiano, que sempre deram uma importância especial à educação. Eles me instruíram e apoiaram para que eu tivesse a mesma visão. São corresponsáveis por eu transformar esse sonho em realidade.

AGRADECIMENTOS

Ao Prof. Dr. Eric Fagotto,
Guia paciente e compreensivo, orientador e incentivador dos meus trabalhos e da minha formação, pelos ensinamentos, atenção, disponibilidade e por acreditar em mim.

À Pontifícia Universidade Católica de Campinas,
Pela concessão da bolsa, fundamental para realização do Mestrado.

À organização na qual trabalho,
Por permitir a utilização dos seus recursos para o desenvolvimento deste trabalho.

Aos colegas e companheiros,
Pelo apoio e toda solidariedade.

Aos Profs. Drs. David Bianchini e Indayara Bertoldi Martins,
Pelas importantes críticas e sugestões.

Ao Sr. Marcelo Mozer,
Pela revisão dos gráficos e indicadores.

“Insanidade é fazer a mesma coisa várias e várias vezes e esperar resultados diferentes”.
Albert Einstein
(1879-1955)

RESUMO

FREITAS, Pablo Gulias Rufino de. *Segurança da informação e QoS na gestão de redes de telecomunicações em conformidade com as práticas de ITIL*®. 2017. 87f. Dissertação (Mestrado em Gestão de Redes de Telecomunicações) – Pontifícia Universidade Católica de Campinas, Centro de Ciências Exatas, Ambientais e de Tecnologia, Faculdade de Engenharia Elétrica com ênfase em Telecomunicações, Campinas, 2017.

Tradicionalmente, Segurança da Informação (SI) e Qualidade de Serviço (*Quality of Service* (*QoS)*), que significa a capacidade de um serviço para satisfazer as necessidades do usuário, têm sido consideradas, separadamente, com diferentes propósitos e necessidades. No entanto, os níveis de serviços anunciados e esperados por ambos estão fortemente ligados. Nesse sentido, apesar da melhoria no desempenho da comunicação e da confidencialidade, integridade e disponibilidade dos dados transportados serem premissas maiores, ainda não há uma padronização para um uso conjunto e eficiente entre SI e *QoS*. Também não há uma definição de métricas ou indicadores que possibilitem essa medição agrupada. No presente trabalho, propõe-se e testa-se um modelo de gerenciamento de redes de telecomunicações, baseado nas melhores práticas da biblioteca de Gerenciamento de Serviços de Tecnologia da Informação (GSTI), *Information Technology Infrastructure Library* (ITIL), tendo como novidade a utilização do processo de gestão de riscos de segurança da informação, da norma 27005 (Gestão de riscos), em conjunção com uma lista de verificações de requisitos de QoS e controles da norma 27002 (Código de práticas). Este trabalho busca o equilíbrio entre SI, desempenho e produtividade. Os resultados obtidos mostraram a efetividade da proposta com uma diminuição aproximada de 16%, da quantidade de incidentes diretamente ligados à SI e QoS, detectados e solucionados de forma proativa.

Palavras-chave: ITIL. *Quality of Service*. Segurança da informação. Monitoramento. Monitoração. Melhores práticas. Gerenciamento de serviços. Tecnologia da informação.

ABSTRACT

FREITAS, Pablo Gulias Rufino de. Information Security and QoS in the management of telecommunication networks in conformance with ITIL. 2017. 87f. Dissertation (Masters in Management of Telecommunication Networks) - Pontifícia Universidade Católica de Campinas, Centro de Ciências Exatas, Ambientais e de Tecnologia, Faculdade de Engenharia Elétrica com ênfase em Telecomunicações, Campinas, 2017.

Traditionally, Information Security (IS) and Quality of Service (QoS), which means the capacity of a service to satisfy the needs of a user, have been considered separately, with different purposes and needs. However, the service levels that are advertised and expected for both are strongly linked. In this sense, despite the improvement in the performance of communication and of the confidentiality, integrity and the availability of data trafficked having greater premise, there still is no standardization for the joint and efficient use of IS and QoS. There are also no defined metrics or indicators that allow for this grouped measurement. This study proposed and tested a model for the management of communication networks, based on the best practices of the library for Information Technology Service Management (ITSM), Information Technology Infrastructure Library (ITIL), having the novelty of using the information security risk management process, from the 27005 (Risk Management) standard, in conjunction with a list of requirements checks of QoS and controls from the 27002 (Code of Practice) standard. This study looks to find the equilibrium between IS, performance and productivity. The results obtained showed the effectiveness of this proposal decreasing by approximately 16%, the number of incidents directly linked to IS and QoS, detected and solved in a proactive manner.

Index Terms: ITIL. Quality of Service. Information security. Monitoring. Best practices. Service management. Information technology.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT = Associação Brasileira de Normas Técnicas
AES = *Advanced Encryption Algorithm*
ANS = Acordo de Nível de Serviço
BC = *Business Case*
BIA = *Business Impact Analysis*
CEO = *Chief Executive Officer*
CSF = *Critical success factor*
CIO = *Chief Information Officer*
COBIT = *Control Objectives for Information and Related Technology*
CPU = *Central Processing Unit*
DiffServ = *Differentiated Services Framework*
DIKW = *Data-Information-Knowledge-Wisdom*
DMZ = *Demilitarized Zone*
ERP = *Enterprise Resource Planning*
GSTI = Gerenciamento de Serviços de Tecnologia da Informação
GTB = *Grow the Business*
IEC = *International Electrotechnical Commission*
IETF = *The Internet Engineering Task Force*
IntServ = *Integrated Services Architecture*
IoT = *Internet of Things*
ISO = *International Organization for Standardization*
ITIL = *Information Technology Infrastructure Library*
ITILV3 = *Third version da Information Technology Infrastructure Library*
ITSMF = *Information Technology Service Management Forum*
ITU = *International Telecommunications Union*
KPI = *Key Performance Indicator*
LAN = *Local Area Network*
MPLS = *Multiprotocol Label Switching*
NMS = *Network Management Systems*
OLA = *Operational Level Agreement*
OGC = *Office of Government Commerce*

PDCA = *Plan, Do, Check and Act*

QoS = *Quality of Service*

RACI = *Responsibility Assignment* Matrix

RAO = Relatório Analítico de Obra

RDM = Requisição de Mudança

RTB = *Run the Business*

SGSI = Sistema de Gestão da Segurança da Informação

SI = Segurança da Informação

SIP = *Service Improvement Plan*

SLA = *Service Level Agreement*

SPOC = *Single Point Of Contact*

SQoS = *Security Quality of Service*

SWOT = *Strengths, Weaknesses, Opportunities and Threats*

TCP = *Transmission Control Protocol*

TI = Tecnologia da Informação

TTB = *Transform the Business*

URL = *Uniform Resource Locator*

VPN = *Virtual Private Network*

SUMÁRIO

1 INTRODUÇÃO

A Informação é o significado da aplicação de um contexto a um conjunto de dados, que são fatos discretos. A compreensão dos relacionamentos entre esses fatos, por meio de respostas a uma ou mais das perguntas, do tipo: Quem? O quê? Quando? Onde?, resulta na Informação.

A Figura 1 mostra o Modelo *Data-Information-Knowledge-Wisdom* (DIKW), também conhecido como Pirâmide do Conhecimento, que é formado pelos conceitos de Dados, Informação, Conhecimento e Sabedoria. Esse modelo expõe uma hierarquia resultante da Compreensão *versus* o Contexto, na qual os Dados, com seus números, imagens e palavras, formam o nível mais básico e necessário para alcançar um discernimento ou deduzir as consequências de forma assertiva, a respeito de um acontecimento. A Informação, como explicado anteriormente, acrescenta interpretação e sentido aos Dados. O Conhecimento é a forma de aplicação da Informação, sobre como usá-la de maneira adequada, em função da experiência e capacidade cognitiva do indivíduo. Como último nível hierárquico, a Sabedoria é mais subjetiva, ao procurar antecipar uma situação. Ela necessita dos três conceitos anteriores, além do entendimento, reflexão e inovação sobre o modo de utilizá-los. (FRICKÉ, 2009).

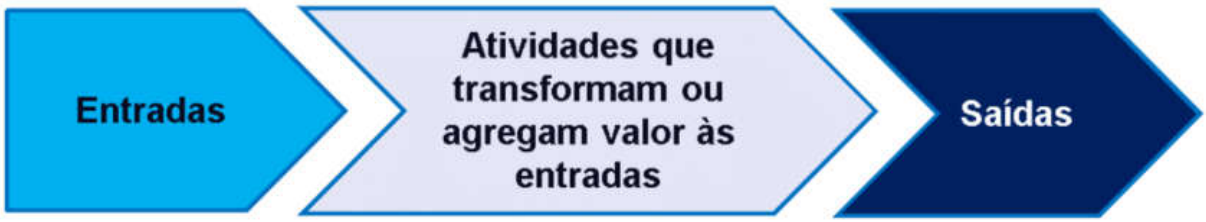
Figura 1. Modelo DIKW adaptado

Fonte: Nürnberger e Wenzel (2011)

A informação é tradicionalmente relacionada aos documentos impressos, quando, de fato, também pode ser verbal ou transmitida e armazenada em meios eletrônicos. É um ativo muito valioso para o negócio da organização. Por esse motivo, faz-se necessária a utilização de recursos tecnológicos, de forma efetiva, para obter o conhecimento que proporcione um diferencial estratégico e competitivo, tendo na variável do custo uma consideração essencial. (PINHEIRO, 2004).

Os processos de negócio são um conjunto estruturado de atividades necessárias para entregar um produto ou serviço, em uma organização. Ou melhor, uma cadeia de tarefas executadas, que converte insumos (entradas) em um resultado com valor agregado (saídas), conforme reproduzido na Figura 2.

Figura 2. Processos de negócio



Fonte: Baars *et al*. (2015)

Basicamente, há três tipos de processos de negócio:

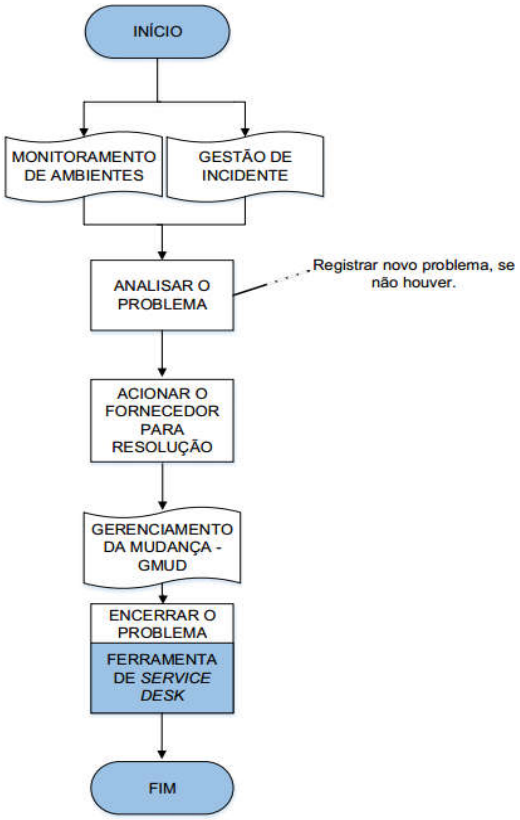
1. Primários – processos que geram receita para a organização;
2. Estratégicos – processos que desenvolvem a estratégia, que apoiam a governança;
3. Suporte – processos que suportam os dois tipos anteriores.

Os processos devem ser funcionais e estar adequados às necessidades do negócio, com o objetivo de garantir o compartilhamento de conhecimento, monitorar e medir as atividades, para a identificação de pontos de melhoria, e de certificar que todas as atividades mapeadas possam ser desempenhadas, de acordo com os critérios de qualidade estabelecidos. Em resumo, esperam-se processos efetivos, que entreguem os serviços solicitados, no menor tempo possível, da melhor maneira possível e sem burocratizar a operação. Assim como a infraestrutura e os sistemas, os processos também precisam de manutenção. Eles devem ser revisados e

readequados às necessidades do negócio, sempre que houver uma mudança de estratégia. (CHIARI, 2014).

Analisando os processos de negócio, é possível observar como uma organização lida com as informações e também com o valor e a importância das mesmas. Há processos que são muito dependentes da disponibilidade da informação, assim como há outros que dependem mais da confidencialidade ou integridade da mesma. A Figura 3 exibe um exemplo de processo utilizado no ambiente de experimentação desse trabalho, quando se faz necessário o acionamento do fornecedor para que seja identificada uma solução para o problema.

Figura 3. Gestão de Problemas



Fonte: Elaborado pelo autor

Os sistemas de informação, no contexto referente à segurança da informação (SI), são um conjunto de meios tecnológicos, procedimentos, regras e pessoas, conforme mostrado na Figura 4, que devem assegurar a confiabilidade das informações aos processos de negócios da organização. Por meio de sistemas de informação é possível transferir, armazenar e processar essas informações.

Figura 4. Sistema de Informação

Fonte: Baars *et al*. (2015)

Os serviços de Tecnologia da Informação (TI) são o meio de entregar valor ao cliente, com o objetivo de atingir os resultados esperados, alinhados com o negócio. Os serviços de TI suportam os processos das áreas de negócio de uma organização, por intermédio de sistemas de informação. Esses serviços devem ser entregues ao cliente de acordo com a qualidade acordada. Essa qualidade é alcançada quando o cliente experimenta o valor agregado ao negócio e, para isso, os serviços de TI precisam apresentar duas características essenciais:

- Garantia – corresponde a um serviço entregue, apto para seu uso, referente aos aspectos de desempenho e segurança;
- Utilidade – diz respeito à percepção positiva do cliente sobre o serviço entregue, apto para seu propósito, referente às funcionalidades que permitam a realização das atividades com melhor desempenho.

Essa entrega torna-se viável, executando as melhores práticas de governança e gerenciamento de serviços de TI, por meio de planejamento, organização e maturidade dos processos organizacionais.

Os serviços de TI possuem um ciclo de vida orientados por processos, distribuídos em 5 estágios. (SELM, 2008). Cada estágio do ciclo de vida do serviço tem influência na criação de valor. De forma resumida, o valor do serviço é modelado na Estratégia de Serviço, a fim de garantir que as necessidades dos clientes sejam

compreendidas. A implementação na forma de serviço, a partir da concepção de um projeto, ocorre nos estágios de Desenho de Serviço e Transição de Serviço. A entrega do serviço, de forma consistente e sustentável, é concretizada na Operação de Serviço, em que o valor é realmente percebido pelo cliente. Ao longo dos estágios anteriores e para garantir que os serviços estejam alinhados às necessidades, deve ser realizado um trabalho contínuo de qualidade por meio do estágio de Melhoria Continuada do Serviço. A Figura 5 apresenta a decomposição e os níveis de associação dos componentes de um serviço de TI. É possível observar que o Sistema de Informação faz parte de um serviço de TI.

Figura 5. Serviços de TI

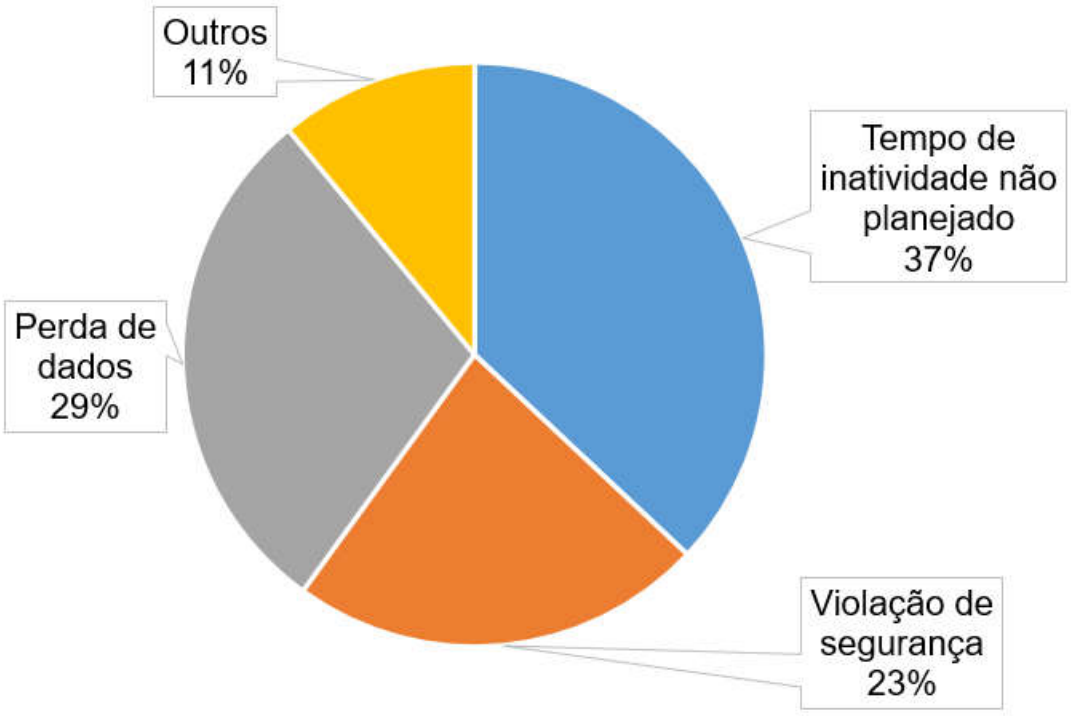
Fonte: Selm (2008)

A área de atuação de TI possui uma abrangência mais ampla que as de informática, processamento de dados, sistemas de informação e telecomunicações, pois envolve também aspectos humanos, administrativos e organizacionais, que influenciam o fluxo de trabalho. (LAURINDO et al, 2001).

A área de TI ocupa uma posição crucial na organização, suportando os processos de negócios, por intermédio de seus serviços. No entanto, existem diferenças significativas nas percepções e expectativas dos líderes de TI e das demais

áreas, em tópicos tão primordiais como a melhoria contínua de serviços e a SI. Para conhecer essas diferentes percepções, foi realizado o estudo global *IT Trust Curve*, composto por 3200 entrevistas em 16 países, sendo 1600 com tomadores de decisão de TI e 1600 com tomadores de decisão de dez segmentos de negócios. Os países participantes foram: Estados Unidos, Brasil, Alemanha, Rússia, Japão, China, Índia, Canadá, Reino Unido, França, Espanha, Itália, Bélgica, Holanda, Luxemburgo, Austrália e África do Sul. Os entrevistados eram funcionários de empresas dos segmentos de ciências biomédicas, serviços financeiros, tecnologia da informação, saúde, setor público, indústria, varejo, energia, mídia, entretenimento e consultoria, com metade trabalhando em organizações com 100 a 1000 funcionários e a outra metade em organizações com mais de 1000 funcionários. A resposta da maioria dos entrevistados (61%) revelou que, nos últimos 12 meses, 3 em cada 5 organizações sofreram prejuízos, devido a uma infraestrutura de TI inadequada. Essa infraestrutura deficitária foi a causa de, pelo menos, um dos seguintes incidentes: tempo de inatividade não planejado (37%), violação de segurança (23%) ou perda de dados (29%), conforme indicado na Figura 6. Bourne (2013).

Figura 6. Incidentes de infraestrutura de TI



Fonte: Elaborada pelo autor

As consequências desses incidentes causaram grandes danos. Os três principais foram a perda de produtividade dos funcionários (45%), a perda de receita (29%) e a perda da confiança/lealdade do cliente (32%), como apontado na Figura 7.

Figura 7. Consequências de uma infraestrutura de TI inadequada para o negócio

Fonte: Bourne (2013)

Diante dos resultados expostos, verifica-se a dificuldade das organizações em obterem mais eficiência na melhoria contínua de serviços de TI e de SI. As diferenças nas percepções e expectativas entre os líderes de TI e das demais áreas de negócios podem ser a explicação e ficam evidenciadas quando:

- Um em cada cinco entrevistados indicou a falta de confiança em tecnologia ou na área de TI, como uma limitação importante para se obter mais eficiência na entrega de serviços de TI e de SI. As outras limitações informadas foram o orçamento, planejamento e as restrições de recursos/carga de trabalho;
- Apenas 50% de todos os tomadores de decisão de outros segmentos de negócios consideram a TI como impulsionador de uma infraestrutura mais flexível e segura, em comparação com a mesma opinião para 70% dos tomadores de decisão de TI;
- No Brasil, 27% dos executivos de TI entrevistados relataram que sofreram falhas de segurança ou deterioração na performance das comunicações, nos

12 meses anteriores, enquanto apenas 19% dos executivos de outros segmentos de negócios relataram ter sido vítimas. Bourne (2013).

Em outro estudo, o *The Global State of Information Security Survey 2016*, realizado pelas publicações americanas CSO e CIO em conjunto com a PricewaterhouseCoopers, com a participação de mais de 10.000 executivos de negócio e de TI, de mais de 130 países, foram estimadas perdas financeiras de US$ 1 milhão, em média, decorrentes de incidentes de segurança, somente nas empresas brasileiras, no ano passado. Nesse sentido, das 486 companhias brasileiras que responderam o questionário, algumas chegaram a registrar um período de inatividade total (indisponibilidade dos serviços, sistemas e rede) por mais de cinco dias, sendo que a maioria (65%) ficou totalmente inoperante entre uma e 24 horas. (COOPERS, 2016).

Neste trabalho propõe-se e testa-se um modelo de gerenciamento de redes de telecomunicações, fundamentado nas melhores práticas da biblioteca de GSTI, ITIL, aplicando o processo de gestão de riscos de segurança da informação, da norma NBR ISO / IEC 27005. Essa aplicação está associada à uma lista de verificações de requisitos de QoS e controles de SI, da norma NBR ISO / IEC 27002. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011b, 2013b). O objetivo é oferecer uma entrega de serviços segura e com qualidade, por intermédio de alertas de monitoramento, com foco em SI e QoS. Para tanto, são realizadas iterações por meio dos processos do modelo proposto com o intuito de, proativamente, reduzir os incidentes vinculados à SI e QoS, que afetam o negócio.

Esta dissertação está desenvolvida em oito capítulos. No Capítulo 2, descrevem-se as fundamentações sobre a TI estratégica, SI e QoS. Essas fundamentações são realizadas com um enfoque prático, a partir de estândares, tendências e pesquisas atuais. No Capítulo 3, expõe-se e discute-se o modelo proposto, por intermédio da planificação, diagrama e processos inerentes. No Capítulo 4, apresenta-se o ambiente utilizado para validação do método. No Capítulo 5, demonstram-se os resultados das implementações realizadas. Finalmente, no Capítulo 6, revela-se a conclusão e os trabalhos futuros.

Algumas palavras originais foram mantidas, uma vez que são jargões utilizados na área, mesmo no Brasil, conforme a tabela que segue:

Tabela 1. Jargões de TI

Jargão de TI	Significado resumido
Arquitecture	Arquitetura
Backup	Cópia de segurança de dados
Balanced scorecard	Ferramenta de gestão para medir o desempenho da empresa
Benchmarking	Processo de comparação de produtos, serviços e práticas
Big data	Processamento de grande volume de dados armazenados
Blade	Servidor otimizado, em formato de lâmina
Buffering	Área para armazenamento temporário de dados
Business case	Caso prático de negócio
Cloud	Computação na nuvem
Critical	Alerta crítico
Dashboards	Painel de controle com informações gerenciais
Data center	Centro de processamento de dados
Delay	Atraso nas transmissões
Disk Drive	Disco rígido (HDD)
Display Name	Nome do dispositivo
Drill down	Recurso para apresentar a informação detalhadamente
Exceptions	Exceções
Firewall	Dispositivo de segurança, para redes de comunicações
Frameworks	Conjunto de conceitos para resolver um problema específico
Hackers	Indivíduos que elaboram e alteram softwares e hardwares
Hardware	Parte física de um computador
Internet	Sistema global de redes de computadores interligadas
IoT	Objetos da vida cotidiana conectados à internet
LAN to LAN	Interconexão direta entre redes locais
Link	Ligação entre dispositivos de comunicação
Logout	Desconectar-se

Major	Alerta importante. Menos importante que o alerta *Critical*
Malware	Programa indesejado e malicioso
Memory	Memória
Monitors	Monitoradas
Operating System	Sistema operacional
Ping	Comando para testar a conectividade entre dispositivos
Ports	Portas
Ransomware	Programa indesejado e malicioso
Server	Servidor
Service Name	Nome do serviço
Sites	Locais ou conjunto de páginas da internet
Software	Parte lógica de um computador
Spyware	Programa indesejado e malicioso
Storage	Dispositivo de armazenamento de dados
Switch core	Elemento de rede concentrador para interconexão de outros
Switch Brocade	Elemento de rede periférico
Swot	Ferramenta utilizada para fazer análise de ambiente
Thresholds	Limite aceitável definido
Unit	Unidade
Up/Down	Acessível/Não acessível
Zero-day	Vulnerabilidade de segurança da informação

Fonte: Elaborada pelo autor

2 REFERENCIAL TEÓRICO

2.1 TI Estratégica e Diferenciada

A área de TI deve ser encarada como uma área estratégica, uma vez que provê os recursos que viabilizam, em conformidade com o contexto atual da sociedade, as atividades do negócio. No entanto, faz-se necessário demonstrar o valor que agrega ao negócio, para que os investimentos sejam patrocinados pela alta gestão. Para isso, necessitam de um planejamento que permita uma utilização eficiente dos recursos, somado ao comprometimento com as estratégias da organização e a consecução dos objetivos e metas definidas. (SILVA; GOMEZ; MIRANDA, 2010).

Atualmente, a área de TI busca um posicionamento estratégico para deixar de exercer apenas o tradicional papel de suporte administrativo. Sua função, cada vez mais, está sendo questionada, pois já não sustenta “somente” as operações de negócio. A TI é responsável por garantir a segurança e desempenho suficientes do ambiente tecnológico, como também permite que se viabilizem novas estratégias e oportunidades.

A área de TI é parte da estratégia de negócio das organizações, mesmo sem elas o saberem. É fácil reconhecer e comprovar seu papel fundamental em organizações de todos os tamanhos e segmentos, pois a maioria de seus processos e de suas informações dependem de sistemas de informação. Nesse sentido, os níveis dos serviços precisam destacar as entregas para o negócio, para que a alta gestão possa perceber que a TI não é apenas uma conta contábil para alocar despesas de tecnologia. A TI também deve ser percebida como um parceiro estratégico, que entende quais são os objetivos a serem logrados pelo negócio, adequando seus serviços para poder atingi-los. Para isso, é fundamental que o entendimento desses objetivos seja permeado pelos diferentes níveis hierárquicos, desde o CEO, passando pelo CIO, até o atendimento do *service desk*, havendo assim uma cadeia de alinhamentos efetivos. (CHIARI, 2014).

Desde simples atuações para resolução de requisições ou incidentes corriqueiros, até um conjunto de equipes responsáveis por decisões críticas para potencializar a produtividade da organização, essa é a verdadeira realidade da área de TI nas organizações. E os motivos para essa evolução são diversos. Com o planejamento corporativo e da área de TI caminhando juntos, a organização começa a se desenvolver e evoluir, beneficiando-se de:

- Maior qualidade dos produtos e serviços desenvolvidos e existentes, com uma maior satisfação do cliente;
- Inovação aos processos e às entregas;
- Embasamento e suporte para tomadas de decisões;
- Melhor direcionamento e reaproveitamento de recursos, realizando uma gestão efetiva;
- Estabelecimento de políticas de tecnologia, que asseguram padrões e reduzem os riscos e custos.

Esses benefícios estão retratados na Figura 8.

Figura 8. Governança de TI

Fonte: ISACA (2017)

Uma parcela considerável dos gastos com tecnologia provém das áreas de negócios e não da área de TI. A TI orientada por negócios tem um claro valor para a organização e o seu papel deve ser construir relacionamentos com as principais partes interessadas, para estar ciente de novos projetos e dos impactos potenciais sobre as operações. A TI possui um vasto conhecimento do negócio, que deve ser conectado e explorado, porque é o meio para viabilizar melhorias, obrigações legais e correções de erros, de todas as áreas de negócio. Por conseguinte, a TI possui uma visão sistêmica mais abrangente tanto dos processos quanto das necessidades. Essa visão possibilita um diagnóstico empresarial, por meio da identificação de gargalos, pontos de atenção, erros recorrentes, retrabalhos e automatização de tarefas. Como consequência, aumenta-se a capacidade de prever situações adversas, assim como o dinamismo e a proatividade nas soluções. Da mesma maneira, reduzem-se os riscos e custos. Essas vantagens aportam qualidade, efetividade, produtividade, inovação e competitividade às necessidades do negócio.

2.2 ITIL e o Gerenciamento de Serviços de TI

A Governança de TI é o conjunto de normas e processos relacionados à utilização de tecnologia da informação, que visa a utilização eficiente dos recursos e o suporte aos processos da organização, possibilitando a execução das atividades de forma alinhada com as estratégias estabelecidas pela alta gestão. Já a Gestão de TI é o conjunto de processos e controles, que fornecem serviços pertencentes ao catálogo da TI. A Gestão de TI é parte integrante da Governança de TI.

É fundamental que os serviços oferecidos pela área de TI sejam de excelência e melhorem continuamente, atestando a evolução da qualidade dos seus processos. Afinal, a qualidade dos serviços entregues é definida pelas expectativas atendidas dos clientes, que levam em consideração custo, prazo, escopo, conteúdo, além da confiabilidade, integridade e disponibilidade da informação. O Gerenciamento de Serviços de TI é o gerenciamento de integração entre pessoas, processos e tecnologias, formando um serviço de TI, que tem por objetivo atender as necessidades dos clientes. Esse serviço deve estar alinhado com a estratégia do negócio, de acordo

com os níveis de serviços estabelecidos entre a área de TI e a as demais áreas. (MAGALHÃES; PINHEIRO, 2007).

O Gerenciamento de Serviços de TI procura entender as necessidades e expectativas do cliente, para procurar atendê-las satisfatoriamente. No entanto, a TI não é apenas uma área de atendimento ou de registro de falhas e dúvidas. Como premissa do GSTI, todas as atividades de TI devem estar conectadas e ser gerenciadas por boas práticas, que sejam traspassadas aos serviços entregues.

Uma biblioteca de boas práticas traz sugestões de uso comprovadamente adotadas e reconhecidas pelo mercado, que não significam regras pré-estabelecidas. São indicações experimentadas e adaptáveis, com lições aprendidas fundamentais para que os objetivos estabelecidos sejam atingidos, sem tropeços desnecessários. Fala-se de *benchmarking*, que considera o que já funcionou ou funciona na concorrência e pode igualmente funcionar na rotina de sua organização. O sucesso não está necessariamente ligado à prática de todo o conteúdo dessas “sugestões”, mas sim ao uso que se faz delas. Boas práticas de mercado, muito mais do que mudanças estruturais, exigem mudanças de cultura e um genuíno comprometimento. ITIL, que significa Biblioteca de Infraestrutura de Tecnologia da Informação (*Information Technology Infrastructure Library*), criada no Reino Unido, em 1989, contém um conjunto de publicações sobre as melhores práticas para gerenciamento de serviços de TI. Esse conjunto de publicações descreve as práticas testadas e validadas por várias organizações em todo o mundo. Em face do exposto, a ITIL é considerada como a mais reconhecida referência de práticas de gerenciamento de serviços de TI, pois oferece um incremento na vantagem competitiva por meio de redução de custos, maior crescimento e agilidade. Proporciona mais eficiência corporativa, por intermédio da racionalização de processos de TI, melhor percepção e valorização da TI e melhor satisfação de clientes e usuários. (AXELOS, 2017).

Embora o acrônimo ITIL se refira a uma biblioteca de infraestrutura de TI, nos quase 30 anos de existência, a ITIL evoluiu e mudou conforme a tecnologia e o desenvolvimento de novos modelos de negócio. Atualmente, *Axelos* é a organização que suporta, desenvolve e dissemina globalmente as melhores práticas da biblioteca ITIL, que é de domínio público. O número de profissionais certificados, somente no

Brasil, é de aproximadamente cem mil. Seus conceitos são tão populares que a converteu em uma referência adotada também pelos mais importantes *frameworks* de governança, como o COBIT e a norma ISO/IEC 20000, que tem como foco certificar a qualidade da prestação de serviços de TI nas organizações. No meio de TI, é comum a utilização das expressões “Incidentes”, “Problemas” e “SLA”, por exemplo.

ITIL contém duas grandes atualizações. A versão atual, V3, aborda uma atualização realizada em 2011, que é composta por cinco publicações principais: Estratégia de Serviço, Desenho de Serviço, Transição de Serviço, Operação de Serviço e Melhoria Contínua de Serviço, com um total de 26 processos e 4 funções.

As atividades de gerenciamento de serviços, em ITIL, são estruturadas com base no ciclo de vida do serviço, desde a sua concepção até a sua descontinuação. Na Figura 9, observam-se os estágios do ciclo de vida do serviço, que se referem aos cinco livros da biblioteca.

Figura 9. Ciclo de vida do serviço adaptado

Fonte: Axelos (2017)

Esses estágios são listados e detalhados em seguida:

1. Estratégia de Serviço;
2. Desenho de Serviço;
3. Transição de Serviço;
4. Operação de Serviço;
5. Melhoria contínua de serviço.

1. Estratégia de Serviço (ITIL *Service Strategy*) – refere-se ao estágio de concepção do serviço, que determina quais tipos de serviços devem ser oferecidos. Segue as definições da direção estratégica dos serviços de TI, em função de quem são os seus clientes e de quais serviços serão disponibilizados para eles, por meio de questões como:

- O que sua organização quer ser?
- Como nós podemos fazer o melhor uso dos serviços para beneficiar a organização?
- Como nós podemos nos diferenciar de outros competidores e criar valor para nossos clientes?

A Estratégia de Serviço permite que o gerenciamento de serviços de TI se torne um ativo estratégico, assegurando uma entrega de serviços focada em suportar as necessidades de negócio. Sendo assim, o provedor decide quais serviços de TI são necessários para apoiar o negócio na consecução de resultados. Uma vez definida a estratégia, são estabelecidas as políticas e padrões para facilitar sua implementação. Após definir quais são os serviços de TI necessários, a Estratégia de Serviço ainda inclui atividades para aprovar os serviços e adquirir o financiamento e recursos para desenvolvê-los. Esses objetivos estratégicos são implementados com a execução de processos, de outros estágios do ciclo de vida do serviço, para desenhar e implementar esses serviços no ambiente de produção. Para depois, passar a gerenciá-los e melhorá-los continuamente. Todas estas questões são detalhadas nos seguintes processos:

- Gerenciamento Estratégico para Serviços de TI;
- Gerenciamento de Relacionamento com o Negócio;
- Gerenciamento de Portfólio de Serviço;
- Gerenciamento Financeiro para Serviços de TI;
- Gerenciamento de Demanda.

Percebe-se que na estrutura estabelecida pela ITIL, a Estratégia é representada no centro da Figura 9. O motivo é simples. Nenhuma iniciativa ou projeto, seja o desenho de um novo serviço ou a adaptação de um processo, faz sentido se não for para trazer benefícios ao negócio.

2. Desenho de Serviço (ITIL *Service Design*) – nesse estágio ocorre o desenho de um novo serviço ou modificação de um existente, tendo em vista sua aplicação no ambiente produtivo. A estratégia do serviço começa a tomar forma e é hora de planejar como a organização vai se transformar, em conformidade com o que foi definido. A partir dos requisitos do negócio, que são estabelecidos no estágio da Estratégia de Serviço, são construídos planos, desenhos e estimativas de recursos. O estágio de Desenho de Serviço incorpora os seguintes processos:

- Coordenação do Desenho;
- Gerenciamento de Nível de Serviço;
- Gerenciamento do Catalogo de Serviços;
- Gerenciamento de Fornecedores;
- Gerenciamento de Disponibilidade;
- Gerenciamento de Capacidade;
- Gerenciamento da Continuidade de Serviços de TI;
- Gerenciamento de Segurança da Informação.

3. Transição de Serviço (ITIL *Service Transition*) – este estágio auxilia a organização a planejar e gerenciar as mudanças em serviços, além de implementar liberações no ambiente produtivo. É aqui onde são construídos e implementados

serviços novos ou modificados. Neste momento é preciso garantir que, o que foi desenhado no estágio anterior se transforme em um serviço disponível, com o menor risco possível. Em outras palavras, esse é o estágio no qual os serviços são materializados em algo “consumível”. A Transição de Serviço se preocupa em garantir que os requisitos da Estratégia de Serviço, incluídos no Desenho de Serviço, sejam efetivamente realizados na Operação de Serviço, controlando os riscos de falhas e interrupções. Os seguintes processos fazem parte desse estágio:

- Planejamento e Suporte da Transição;
- Gerenciamento de Mudança;
- Gerenciamento de Configuração e Ativos de Serviço;
- Gerenciamento de Liberação e Implantação;
- Gerenciamento do Conhecimento.

4. Operação de Serviço (ITIL *Service Operation*) – neste estágio são coordenadas e executadas as atividades e processos necessários para entregar os serviços aos clientes e usuários do negócio. Esses serviços são gerenciados em conformidade com os níveis acordados. Uma vez disponibilizado o serviço, é o momento de garantir que este funcione, de acordo com o que foi previsto na Estratégia de Serviço, com o mínimo de interrupções e com o tratamento adequado para os imprevistos. A Operação de Serviço também envolve o gerenciamento de rotina, da tecnologia usada para entregar ou suportar os serviços. Os serviços de TI passam a ser consumidos pelos clientes e usuários. Em outras palavras, é neste estágio onde o valor do serviço é percebido. Seus processos incluem:

- Gerenciamento de Eventos;
- Gerenciamento de Incidentes;
- Cumprimento de Requisição;
- Gerenciamento de Problemas;
- Gerenciamento de Acesso.

A abrangência deste estágio vai além do escopo operacional do dia a dia, com a entrega de serviços para criar valor. Existem outros desafios importantes, que oferecem riscos à criação de valor, como os custos do gerenciamento de serviços, quando já estão em produção e que comumente não são incluídos na fase de planejamento do projeto. É muito mais fácil identificar custos de um projeto, do que quantificar quanto um serviço custará após alguns anos de operação.

5. Melhoria de Serviço Continuada (ITIL *Continual Service Improvement*) – o propósito desse estágio é realizar o alinhamento constante dos serviços de TI, de acordo com as necessidades do cliente. Esse alinhamento é realizado, identificando e implementando as melhorias aos serviços de TI que suportam os processos de negócio. Dessa forma, aprende-se dos sucessos e fracassos do passado e melhoram-se continuamente a competitividade e efetividade dos serviços e processos. Por esse motivo, há uma preocupação em garantir que todo o ciclo de vida do serviço passe por uma avaliação criteriosa. Em linhas gerais, as atividades de melhoria contínua de serviço são:

- Identificar, ou ajudar a identificar oportunidades de melhoria;
- Priorizar as melhorias identificadas;
- Definir e executar, ou ajudar a definir e executar, iniciativas de melhoria.

Como pontos de atenção, para possibilitar uma implantação bem-sucedida de práticas de gerenciamento de serviços, a ITIL enfatiza a necessidade de um forte patrocínio da alta gestão, pois é uma iniciativa que envolve mudança cultural. Assim como, apesar de sua popularidade, nem todas as respostas e abordagens estão disponíveis na ITIL. Ela contém alguns processos e modelos, mas não é uma metodologia e não contém todos os detalhes de uma implementação. Não há regras impondo que tudo deva ser implementado. Em ITIL “tudo pode”, desde que seja adotado, para ser adaptado.

A área de TI passa a ter uma visão mais conectada às necessidades do negócio e mais proativa quanto à utilização dos recursos tecnológicos e a prestação

de serviços. Melhora-se, desta forma, a satisfação do cliente e a motivação da equipe de TI, por meio de uma abordagem mais profissional para a prestação de serviços.

Na Tabela 2, estão especificados os processos e funções da biblioteca ITIL, contendo os principais documentos concebidos.

Tabela 2. Processos e Funções da biblioteca ITIL adaptado

Etapas	Descrição	Processos	Documentos Chave
Estratégia de Serviço	Determinar perspectiva / Formar uma posição / Planejar e executar planos / Adotar padrões de ações	Gerenciamento de: Estratégia para Serviços de TI / Portfólio de Serviços / Riscos e de Relacionamento de Negócios / Demanda	Visão e missão / Planos e políticas estratégicas / Serviços: Requisitos, objetivos, modelos, pacotes, definições e classificações / Análise de impacto de negócios (BIA) / Definição das partes interessadas
Desenho de Serviço	Planejar e preparar / Coletar requisitos / Projetar / Analisar e revisar o desenho / Avaliar soluções alternativas / Adquirir e/ou desenvolver	Gerenciamento de: Catálogo de Serviços / Capacidade (negócio, serviço e dispositivo) / Disponibilidade (reativo e proativo) / SI / Nível de Serviço / Fornecedores / Continuidade de Serviços de TI	Definições e catálogos de serviços / Processos; Medidas e métricas / Acordos de nível de serviço (SLA) e acordos de nível operacional (OLA) / Plano de melhoria do serviço (SIP) / Política de disponibilidade, planos, critérios de desenho, análise de risco e relatórios / Política de capacidade, planos, análise de carga de trabalho, previsões e relatórios / Política de negócios e SI, estratégia, planos, análise de risco, classificação, controle e relatórios / Política de continuidade de negócios e serviços de TI, estratégia, planos, risco e análise de impacto de negócios e relatórios / matriz RACI

Transição de Serviço	Planejar e preparar / Construir e testar / Treinar e pilotar / Transferir, instalar e retirar / Revisar e encerrar	Gerenciamento de: Liberação e Implantação / Suporte e Planejamento de Transição / Conhecimento / Mudança / Configuração e Ativo de Serviço	Linhas de base de configuração, relatórios de status e de Auditoria / Políticas de liberação, planos, pacotes e documentação / Política de qualidade de serviço, política de risco e erros conhecidos / Criar planos, documentação e relatórios de avaliação e implantação
Operação de Serviço	Monitorar e controlar / Gerenciar serviços, componentes e atividades / Gerar métricas / Fornecer relatórios / Funções: *Service desk;* Gerenciamento de operações de TI; Gerenciamento técnica; Gerenciamento de aplicação.	Gerenciamento de: Acesso / Eventos / Incidentes / Problemas / Cumprimento de Requisição	Políticas e planos de operação de serviço / Requisitos operacionais, de Gerenciamento de eventos, incidentes, problemas, cumprimento de solicitação e SI / Procedimento de incidente maior / Documentação / Processos, procedimentos operacionais e instruções
Melhoria Contínua de Serviço	Planejar / Fazer / Checar / Agir	Gerenciamento de Melhoria em 7 passos / Técnicas comuns de Melhoria / Gerenciamento de Serviço / Serviço de Relatórios e Indicadores	Políticas e planos de Melhoria de Serviço Continuada / Fatores Críticos de Sucesso (CSFs) / Indicadores chave de desempenho (KPIs) e métricas e realizações / Metas de nível de serviço e realizações / *Balanced scorecard* / Planos de Melhoria de Serviços (SIPs) / *Business Cases* (BCs) / Análise de *SWOT* / Relatórios e *dashboards* de serviço

Fonte: Elaborada pelo autor

2.3 Segurança da Informação (SI)

As informações sigilosas são cruciais para um negócio e devem ser cuidadas com o máximo de rigor possível, pois afetam a competitividade da empresa.

A Segurança da Informação (SI) possui como propriedades básicas, que definem os aspectos de confiabilidade da informação, o tripé CID: **C**onfidencialidade, **I**ntegridade e **D**isponibilidade (BAARS *et al*., 2015), descritos a seguir:

- **Confidencialidade**: é a propriedade de a informação estar acessível somente a indivíduos, entidades ou processos autorizados. Suas principais características são:

    - Exclusividade – os dados estão disponíveis exclusivamente para usuários e processos autorizados a acessá-los;
    - Privacidade – corresponde à limitação do acesso, às informações pessoais.

- **Integridade**: é a propriedade de exatidão e completeza dos ativos da informação. Somente modificações autorizadas podem ser realizadas. Suas principais características são:

    - Autenticidade – a informação é proveniente de uma fonte anunciada e não sofreu alterações ao longo de um processo;
    - Não repúdio – refere-se à impossibilidade de negar a autoria de uma transação realizada.

- **Disponibilidade**: a informação deve estar acessível e utilizável, sempre que necessário, ou demandada por uma entidade autorizada. Suas principais características são:

    - Prontidão – significa a disponibilidade da informação quando necessário;

- Continuidade – remete ao restabelecimento da informação em caso de falha;
- Robustez – representa a capacidade suficiente para garantir a disponibilidade.

Está-se diante da "quarta revolução industrial", na qual as transformações digitais ocorrem em velocidades exponenciais, apoiadas em tecnologias de informação e comunicação. Um período repleto de criatividade, inovação colaborativa, disrupções tecnológicas e criação de modelos de negócios transformadores em todos os segmentos de mercado. Ao mesmo tempo, um mundo cada vez mais digital também apresentará novos desafios e riscos desconhecidos. (PROOF, 2016).

A transformação digital promovida pelas plataformas sociais, *cloud*, IoT, *Big Data* e mobilidade gera oportunidades, como também aumenta a vulnerabilidade. Consequentemente, o risco de ataques cibernéticos são mais frequentes, complexos e nocivos. Os ataques cibernéticos são denominados cibercrime, que são quaisquer atividades ou práticas ilícitas na internet, como invasões de sistemas, roubos de dados, propagações de vírus, entre outras ações maliciosas. Anualmente, as ações do cibercrime causam prejuízos globais na ordem de quatrocentos bilhões de dólares, com um crescimento superior ao vinte por cento, perdendo apenas para o tráfico de drogas e armas. Esses prejuízos são causados pela digitalização dos negócios. A Figura 10 mostra o crescimento anual, contínuo, dos incidentes de SI, apontando as vulnerabilidades, ameaças e riscos, aos quais as organizações estão expostas.

Figura 10. Vulnerabilidades, ameaças e riscos

Fonte: Proof (2016)

A Symantec descobriu mais de 430 milhões de novas instâncias de *malware* em 2015, o que representou um aumento de 36% em relação ao ano anterior. Isso significa que foram criados 1 milhão e 179 mil *malwares* por dia. No final de 2015, o mundo sofreu a maior violação de dados já divulgada publicamente. Um número impressionante de 91 milhões de registros foram expostos. Nesse mesmo ano, o número de vulnerabilidades *zero-day*, que é uma falha de segurança não explorada nem documentada e sem correção conhecida pelo próprio fabricante de *software* ou quaisquer soluções de segurança, mais do que dobrou. Foi um aumento de 125% em relação ao ano anterior. Em outras palavras, em média, uma nova vulnerabilidade de *zero-day* é encontrada a cada semana. As vulnerabilidades podem aparecer em quase qualquer tipo de *software*, mas o alvo mais cobiçado pelos os atacantes é o software amplamente utilizado. Em 2015, as grandes empresas que sofreram ataques cibernéticos amargaram uma média de 3,6 ataques bem-sucedidos. Nos últimos cinco anos, foi observado um aumento constante nos ataques dirigidos a empresas com menos de duzentos e cinquenta funcionários, com 43% de todos os ataques dirigidos a pequenas empresas em 2015, confirmando que, independentemente do tamanho, todas estão em risco. O *ransomware*, que significa o uso da criptografia para manter, como reféns, os dados críticos das empresas e dos indivíduos, foi a grande ameaça de 2016, se destacando por seu alto nível de sofisticação e, principalmente, por sua finalidade exclusiva de extorsão financeira. (PROOF, 2016).

O estudo *The Global State of Information Security Survey 2016*, mostrou também que o número médio de incidentes de segurança reportados nos últimos 12 meses, no Brasil, aumentaram 274%. Esse número é muito superior aos 38% de aumento na média global. Em decorrência desse aumento, 39% dos entrevistados no Brasil apontaram perdas financeiras contra 25% no resto do mundo. (COOPERS, 2016).

Todo negócio possui riscos, e atacantes ávidos por lucro podem ser tão sofisticados tecnicamente como qualquer organização privada ou governamental. O usuário é o elo mais fraco e um ataque a qualquer dispositivo que se conecte com a rede de informações da empresa, seja um computador, celular ou impressora, representa uma ameaça real para toda a rede. A falta de noção e educação

necessárias, em relação às boas práticas de SI, abrem diversas vulnerabilidades para os *hackers* adentrarem no ambiente das organizações.

Nesse cenário de grandes possibilidades e incertezas, o conhecimento e a experiência em SI passam a ter um papel fundamental e de alta visibilidade, porque é relevante no controle de riscos e impactos diretos ao negócio, bem como na rentabilidade de seus produtos e serviços. (PROOF, 2016). A proteção das empresas começa pelo combate à ideia de que a segurança é apenas um custo adicional de TI, quando na verdade, esse “custo” é um investimento dos mais importantes, pois pode evitar graves prejuízos administrativos, financeiros e à imagem e reputação da organização, além de possibilitar a criação de vantagens competitivas e de soluções que facilitem o crescimento do negócio.

Em um mundo interconectado, a informação, os processos relacionados, sistemas, redes e pessoas envolvidas são ativos importantes, que têm um alto valor para o negócio da organização e, como resultado, requerem proteção contra os possíveis riscos. Como parte integrante dos ativos, estão os ativos da informação. Esses ativos são componentes humanos, tecnológicos, físicos e lógicos, que sustentam os processos de negócio.

É de fundamental importância estabelecer diretrizes sobre SI, que estejam adequadas às necessidades e à proteção legal do negócio e de seus empregados. As diretrizes podem estar em forma de políticas, normas, processos, procedimentos e funções de *software* e *hardware*. Essas diretrizes devem promover padrões de comportamento e de uso, referentes aos ativos da informação, como *softwares*, *hardwares*, *internet*, sistemas corporativos, controle de acessos, gestão de ativos, criptografia, classificação da informação, relacionamento com terceiros, conformidade, segurança física e segurança em recursos humanos, operações e comunicações.

Por meio da implantação de controles, que são as implementações das diretrizes, é possível mitigar vulnerabilidades. Dessa forma, previne-se a perda de dados, assegura-se a privacidade, protege-se a propriedade intelectual, minimizam-se prejuízos financeiros, garante-se a continuidade do negócio e maximiza-se o retorno de investimentos em novas oportunidades de negócio.

Para suprir essas carências e apoiar a efetivação dos controles pertinentes, foi projetada a norma NBR ISO / IEC 27002. Essa norma é uma referência na seleção de controles, para as organizações utilizarem no processo de implementação de um SGSI ou como um documento de orientação para as organizações implementarem controles de SI comumente aceitos. A SI é realizada por meio da implementação de um conjunto adequado de controles, que precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b).

Contudo não para por aí, porque a família ISO / IEC 27000 compreende um conjunto com mais de 40 normas, que ajudam a reduzir a exposição de uma organização aos riscos relacionados à SI, por meio de um Sistema de Gestão da Segurança da Informação (SGSI).

A norma NBR ISO / IEC 27001 foi concebida para prover requisitos, com o objetivo de estabelecer, implementar, manter e melhorar continuamente um SGSI. O SGSI tem o objetivo de preservar a confidencialidade, integridade e disponibilidade da informação, por meio da aplicação do processo de gestão de riscos, transmitindo confiança para as partes interessadas. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a).

Na norma NBR ISO / IEC 27005 faz-se necessária uma abordagem sistemática de gestão de riscos, para identificar as necessidades da organização em relação aos requisitos de SI. Dessa forma, cria-se um SGSI eficaz. Essa abordagem deve estar adequada ao ambiente da organização e em permanente alinhamento com o processo principal de gestão de riscos corporativos. Os esforços em segurança buscam combater os riscos de maneira efetiva, no tempo apropriado e onde e quando for necessário. A gestão de riscos de SI deve ser parte integrante das atividades de gestão de SI. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011b).

Já a norma NBR ISO / IEC 27032 fornece diretrizes para aprimorar e potencializar a Segurança Cibernética, planejando e concebendo os aspectos típicos desta atividade. Mais especificamente, essa norma provê um processo mais seguro para a troca de informações, mediante orientações de segurança e a colaboração entre as partes interessadas, para reduzir os riscos da *internet*. Essa norma facilita a

colaboração segura e confiável para proteger a privacidade das pessoas, ajudando a detectar, monitorar e responder aos ataques, a fim de identificar, *hackers*, *malware*, *spyware* e outros *softwares* indesejados. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2015).

É possível afirmar, que a tecnologia será incorporada plenamente aos negócios, integrando as pessoas, coisas e serviços de uma forma cada vez mais inteligente e digitalizada, possibilitando um mundo com experiências digitais que serão tão básicas e relevantes como a luz elétrica é, atualmente. (PROOF, 2016).

> Acreditamos que os dados são um fenômeno do nosso tempo. É o novo recurso natural do mundo. É a nova base de vantagem competitiva e está transformando todas as profissões e indústrias. Se isso tudo é verdade, então o cibercrime, por definição, é a maior ameaça para todas as profissões, indústrias e empresas do mundo. (ROMETY, 2015).

2.4 QoS – *Quality of Service*

Segundo Kurose, Ross e Zucchi (2010), a Internet, por intermédio da comutação de dados e do protocolo de camada de rede, IP, fornece o modelo de serviço do tipo “melhor esforço” (*best effort*), para o envio de dados, porém sem garantia. Não é garantida a entrega nem a ordem e, tão pouco, a integridade (serviço não garantido). Os protocolos de transporte TCP e UDP checam a integridade, mas somente o TCP, que usa os serviços do protocolo IP, promovem uma transferência garantida (serviço garantido). A transmissão dos dados é concorrente e os recursos de rede não são reservados. Quando há congestionamentos, os dados são armazenados e aguardam liberação, sofrendo atrasos e deteriorando o desempenho das comunicações. No entanto, com a implantação de QoS é possível oferecer maior desempenho e segurança para os diferentes tipos de aplicações, e suas respectivas variações nos tipos de tráfego, garantindo o serviço oferecido e a sua utilidade ao usuário. Conforme explicado anteriormente, Garantia (desempenho e segurança) e Utilidade (percepção positiva do cliente) são as duas características que compõem a Qualidade de um serviço entregue.

QoS refere-se à capacidade de uma rede para fornecer serviços otimizados e mais previsíveis para o tráfego de dados. (ALBUQUERQUE, 2013). QoS é a

totalidade das características de um serviço de telecomunicações, que determinam sua capacidade para satisfazer as necessidades explícitas e implícitas do usuário desse serviço. (ITU, 2017). A entrega de um serviço diferenciado ocorre por meio do cumprimento de requisitos das diferentes aplicações. Esses requisitos, que são básicos de QoS, consistem em:

- **Largura de banda ou vazão** – medida da capacidade de transmissão de um meio, determinando a velocidade de transferência dos dados;
- **Atraso, retardo ou latência** – tempo consumido para um pacote de dados alcançar o ponto final de recebimento, após ser transmitido;
- **Variação de atraso ou flutuação do tempo de transmissão (*jitter*)** – variação no tempo e na sequência de entrega dos pacotes de dados;
- **Perda de pacotes de dados** – medida relativa do número de pacotes de dados que não foram recebidos em comparação com o número total de dados transmitidos. A perda de pacotes é tipicamente uma função da disponibilidade e define a Confiabilidade, que está relacionada à baixa perda de pacotes de dados transmitidos.

A Figura 11 exemplifica os requisitos de QoS, de acordo com as diferentes aplicações.

Figura 11. Requisitos de QoS

aplicação	confiabilidade	atraso	*jitter* (variação atraso)	banda
correio eletrônico	alta	baixa	baixa	baixa+
transf. arquivos	alta	baixa	baixa	média+
web	alta	média	baixa	média
login remoto	alta	média	baixa	baixa
audio sob demanda	baixa	baixa	alta	média
video sob demanda	baixa	baixa	alta	alta
telefonia	baixa	alta	alta	baixa
videoconferência	baixa	alta	alta	alta

Fonte: Szigeti *et al*. (2013)

Com QoS, a entrega dos dados é realizada por meio de transmissões fim a fim. Em outras palavras, os pacotes de dados são transmitidos a partir de uma origem e devem ser entregues em um destino predeterminado, percorrendo os elementos de rede envolvidos nessa comunicação. Assim sendo, os requisitos de QoS que devem ser monitorados, não estão em um único elemento, o que dificulta a implementação de QoS.

As redes de comunicações constituem a base de qualquer organização. Por essas redes transitam tráfegos de todo tipo, incluindo voz em tempo real, vídeo de alta qualidade e dados sensíveis a atrasos. Por conseguinte, as redes devem fornecer serviços presumíveis, mensuráveis e, muitas vezes, garantidos, por meio do gerenciamento da Perda de pacotes de dados, Largura de banda, Atraso e sua Variação (*jitter*). (HATTINGH; SZIGETI, 2004).

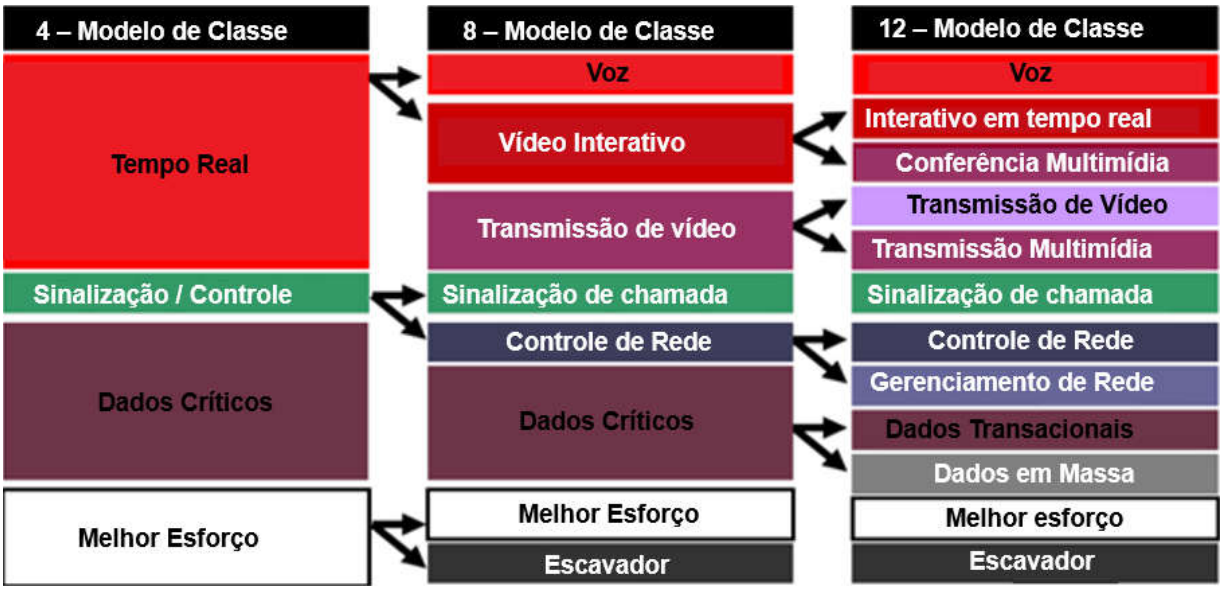
Os principais problemas relacionados à QoS são: pacotes descartados ou perdidos, atrasos na entrega (*delay*), entrega desordenada e erros de envio ou corrupção. Segundo Albuquerque (2013), para mitigar esses problemas são utilizadas as tecnologias de QoS, visando a alocação de recursos, seleção do tráfego e priorização de pacotes. Essas tecnologias referem-se ao conjunto de ferramentas e técnicas, que têm como objetivo a convergência de voz, vídeo e dados de forma transparente, aos usuários finais. As aplicações críticas de voz, vídeo e dados podem receber serviços prioritários ou preferenciais de elementos de rede, de modo que a qualidade dessas aplicações estratégicas não se degrade, a ponto de não serem utilizadas. Essas tecnologias não são apenas úteis na proteção de tráfego desejável, mas também no fornecimento de serviços para o tráfego indesejável, como a propagação exponencial de softwares maliciosos, mediante o monitoramento de fluxos anormais, indicativos de tais ataques.

As técnicas de QoS têm o objetivo de atender as recomendações básicas da organização internacional de telecomunicações, *International Telecommunications Union* (ITU), relacionadas ao desempenho, segurança, confiabilidade e facilidade de manutenção do serviço. Essas técnicas não são concorrentes nem exclusivas. As principais técnicas utilizadas são:

- **IntServ** – a qualidade de serviço é garantida por meio de mecanismos de reserva de recursos. Oferece uma infraestrutura robusta com bastantes recursos, além de uma margem de segurança. É simples e eficaz, mas onerosa;
- **DiffServ** – a qualidade de serviço é garantida por meio de mecanismos de priorização de pacotes de dados. Não é utilizado nenhum mecanismo de reserva de recursos;
- **MPLS** – técnica mais orientada para a modelagem do tráfego de pacote de dados, que para uma garantia de QoS. Simplifica o roteamento realizado pelos elementos de rede, reduzindo suas latências;
- **Dimensionamento** – os elementos de rede são dimensionados durante a fase de projeto, de modo que não haja congestionamentos;
- ***Buffering*** – técnica de armazenamento dos dados à medida que chegam, e sua disposição de acordo com a ordem de envio. (WETHERALL; TANENBAUM, 2011).

À medida que as necessidades dos negócios evoluem, as exigências sobre as tecnologias de QoS também aumentam. A implantação de QoS deve ser planejada em uma abordagem que atenda todas as necessidades. Uma implantação de QoS exitosa é composta por algumas fases, incluindo a definição estratégica dos objetivos de negócios a serem alcançados por meio de QoS, a análise dos requisitos das classes de tráfego a serem provisionadas e o monitoramento dos níveis de serviço. Na Figura 12, exibe-se um modelo, que fornece recomendações respaldadas pelos padrões da organização *The Internet Engineering Task Force* (IETF), para garantir e simplificar essa implantação.

Figura 12. Evolução do modelo de classe de serviço QoS adaptado



Fonte: Szigeti *et al*. (2013)

O modelo possui 12 classes, no entanto, antes da implantação de QoS, a empresa precisa definir claramente os seus objetivos organizacionais, que determinarão quantas classes de tráfego serão necessárias. (SZIGETI *et al*., 2013).

É extremamente importante reconhecer que, mesmo com a implantação de todas as classes de QoS, os impactos dos ataques de negação de serviço são apenas atenuados. Esse tipo de ataque ocorre quando um volume imenso de solicitações é enviado de forma automática a um *site*, serviço, rede ou computador, provocando uma sobrecarga, que gera lentidão ou indisponibilidade. Portanto, a utilização de soluções de segurança, como *firewall* e sistema de detecção de intrusão, são de vital importância para que sejam mantidos os níveis de serviço.

No capítulo seguinte será apresentado o modelo proposto e também será explicado o como e o porquê de sua concepção.

3 MODELO DE GESTÃO DE REDES DE TELECOMUNICAÇÕES UTILIZANDO ITIL, SI E QoS

O escopo desse trabalho é limitado ao gerenciamento de redes de telecomunicações, baseado em ITIL (AXELOS, 2017), no qual é explicada uma metodologia que relaciona os incidentes, problemas, requisições, fluxos, processos e alertas de monitoramento. A ausência de um protocolo estandardizado, que utilize as propriedades de SI e os requisitos de QoS nos dados transportados, motivou a implementação do modelo proposto, que tem a expectativa de reduzir custos e aumentar a produtividade. Outro incentivo para o modelo foi a possibilidade de identificar protótipos desenvolvidos apenas para fins específicos, como o SQoS, para evitar ataques de falsificação de QoS, por exemplo. (SAKARINDR *et al*., 2005).

Na Figura 13 apresenta-se a planificação do modelo proposto, no qual é possível observar as relações existentes entre ITIL, SI e QoS, por meio da interseção ~~comum~~ entre as três áreas. Essa interseção ~~em comum~~ indica os estágios do ciclo de vida do serviço, as diretrizes, os controles, as técnicas e os requisitos que têm influência direta no funcionamento do modelo.

Figura 13. Planificação do modelo proposto

Fonte: Elaborada pelo autor

Ainda sobre a Figura 13, e demonstrando a associação entre ITIL, SI e QoS, são mostrados *frameworks*, normas, modelos e metodologias, por um lado, organizações e certificadoras, por outro, além de ferramentas referentes de *service desk* e monitoramento, relacionadas ao modelo. Para facilitar o entendimento ao longo do trabalho, as imagens relacionadas à ITIL, SI e QoS são representadas nas cores verde, laranja e azul, respectivamente.

Seguidamente e em conformidade com Chiari (2014), são analisados os estágios do ciclo de vida do serviço, que dão nome aos livros da ITIL. **Esses estágios especificam processos que denotam um vínculo direto entre SI e QoS.** Esta simbiose é determinante, uma vez que o resultado final persegue a entrega de um serviço com segurança e qualidade.

No estágio de **Estratégia de Serviços de TI**, por meio da definição de valor do Serviço e da gestão da expectativa, ocorrem as escolhas de requisitos gerais para os serviços que impactam nos critérios de segurança, capacidade e desempenho do serviço. Respectivamente, a definição de valor e a gestão da expectativa fazem parte dos processos de Gerenciamento de Portfólio de Serviços e de Gerenciamento de Relacionamento com o Negócio.

No estágio de **Desenho de Serviço**, os requisitos de segurança e rendimento são definidos como atributos. As atividades proativas dos processos de Gerenciamento de Capacidade e de Gerenciamento de Disponibilidade favorecem a eficiência e a disponibilidade, que são um dos aspectos fundamentais de confiabilidade da informação e afeta diretamente o desempenho. O processo de Gerenciamento de Continuidade para Serviços de TI é uma seção da norma NBR ISO / IEC 27002 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b), que, juntamente com a NBR ISO / IEC 27001, são referências para a ITIL nessa matéria. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a). Do mesmo modo, o processo de Gerenciamento de Segurança da Informação resume a aplicação das boas práticas para a gestão de SI. O processo de Gerenciamento de Fornecedores deve ser utilizado para o cumprimento de acordos com terceiros, que abrangem as propriedades de SI e performance dos serviços entregues. As boas práticas do processo de Gerenciamento de Nível de Serviços são essenciais para melhorar continuamente os

níveis dos serviços e processos atrelados, pois envolvem metas, regras e acordos internos e externos. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011a). Assim sendo, o desempenho esperado do serviço e a confidencialidade, integridade e disponibilidade da informação são influenciados por essas boas práticas.

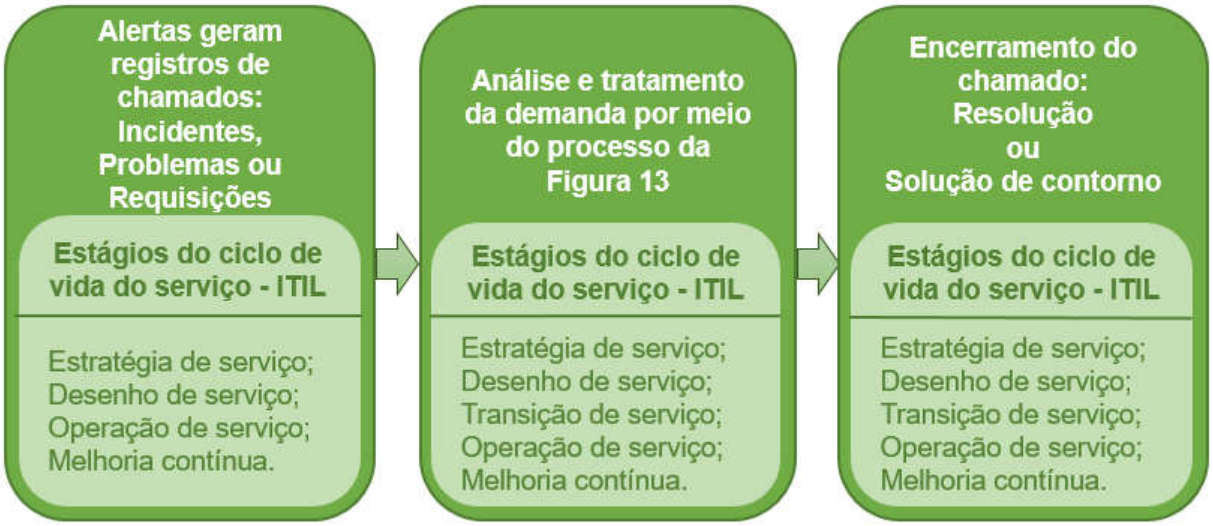
No estágio de **Transição de Serviços**, os requisitos de segurança devem ser contemplados nas especificações de sistemas e infraestrutura, para os processos de Gerenciamento de Liberação e Implantação e Gerenciamento de Mudanças. Como consequência, procura-se analisar os impactos para garantir o rendimento do serviço a ser entregue.

No estágio de **Operação de Serviços**, os tipos de incidentes devem considerar também os incidentes de SI, como um tipo específico, pertencente ao processo de Gerenciamento de Incidentes. No processo de Gerenciamento de Acesso, as regras de acesso são definidas no planejamento que ocorre nos processos de Gerenciamento de Segurança da Informação, Gerenciamento de Capacidade e Gerenciamento de Disponibilidade.

Finalmente, por meio da **Melhoria de Serviços Continuada** são identificados os pontos a serem aperfeiçoados e otimizados nos processos, e que têm influência sobre a SI e QoS. O cumprimento desse estágio é imprescindível e deve ocorrer durante os estágios anteriores, como um trabalho contínuo de qualidade.

A interseção entre ITIL, SI e QoS, que é mostrada na Figura 13, motivou a construção do diagrama apresentado na Figura 14. Essa figura remete ao modelo e ao seu funcionamento, por meio de melhores práticas da ITIL, responsáveis pela gerência de cada um dos blocos apresentados. Nesses blocos observam-se os estágios do ciclo de vida do serviço, que estabelecem as diretrizes dos processos executados.

Figura 14. Diagrama do modelo proposto

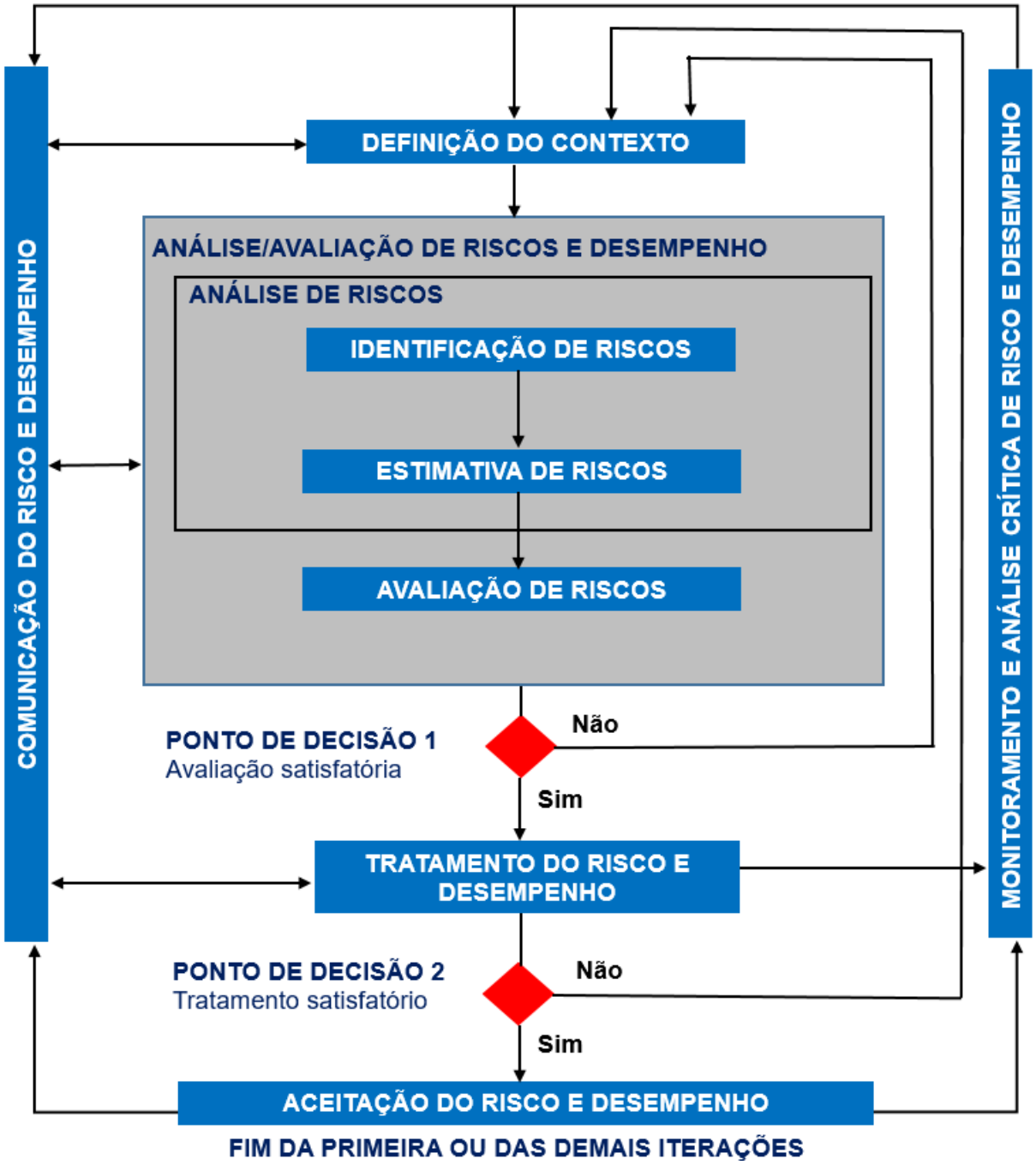


Fonte: Elaborada pelo autor

Resumidamente, o primeiro bloco é a entrada do modelo, no qual são registrados os chamados que dão início às ações do segundo bloco. Basicamente, os registros que alimentam o modelo são provenientes de alertas. O primeiro bloco não possui o estágio Transição de serviço, pois neste estágio os serviços são criados ou modificados. Já no segundo bloco, ocorrem as definições, análises, avaliações, tratamentos e aceitações, por intermédio das iterações que serão explicadas em seguida, na Figura 15. Finalmente, no terceiro bloco, por meio de uma resolução definitiva ou solução de contorno, ocorre o encerramento do chamado. Os procedimentos executados, que resultam no encerramento do chamado, são a saída do modelo.

A etapa principal do modelo ocorre no segundo bloco da Figura 14. Nessa etapa são executados os ~~principais~~ procedimentos para solucionar os chamados registrados. Esses procedimentos são examinados com mais profundidade na Figura 15, na qual também é mostrada a influência que o processo de gestão de riscos tem na relação entre SI e QoS. Esse processo é baseado na norma NBR ISO / IEC 27005, de Gestão de riscos de segurança da informação, e~~,~~ precisa ser contínuo, com o envolvimento das partes interessadas. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011b).

Figura 15. Processo de Gestão de riscos de segurança da informação adaptado



Fonte: Elaborada pelo autor

Neste processo, define-se o cenário no qual a organização está inserida. Em seguida, identificam-se as ameaças que possam significar riscos, avaliando-os em função das consequências indesejadas ao negócio e da probabilidade de ocorrência. Se a avaliação for satisfatória, são fornecidas informações suficientes para que se

determinem as ações necessárias que reduzam os riscos a um nível aceitável. Então, são realizados os procedimentos da lista de verificações, apresentada no APÊNDICE A – Lista de verificações de requisitos de QoS e controles de SI. Essa lista associa os controles de SI com os requisitos de QoS, e sugere ações de acordo com as ocorrências identificadas. Se os procedimentos não forem suficientes, ou seja, se o tratamento não resultar em um nível de risco residual aceitável, ocorre outra iteração do processo, desde o início, com a revisão do contexto, como por exemplo: dos critérios de avaliação de riscos, de aceitação do risco ou de impacto. Frequentemente, são executadas duas ou mais iterações, o que torna possível aprofundar a avaliação em cada repetição. Assim sendo, assegura-se que os riscos de alto impacto ou de alta probabilidade sejam adequadamente avaliados, facilitando a identificação dos controles aplicáveis. Periodicamente, deve haver um monitoramento e uma análise crítica de todo o processo ~~como um todo~~.

A seguir, é apresentado o detalhamento das etapas que formam esse processo. A entrada de cada etapa identifica as informações necessárias para realizar a atividade. A saída identifica as informações resultantes da execução da atividade e pode implicar na entrada da próxima etapa, caso a condição seja positiva.

- DEFINIÇÃO DO CONTEXTO – refere-se ao cenário no qual a organização busca atingir seus objetivos e destaca os elementos característicos que definem sua identidade. O Contexto pode ser de dois tipos:

    - Interno – inclui a estrutura organizacional, cultura, políticas, estratégias, propósitos, normas, fluxos, processos e sistemas de informação;
    - Externo – inclui o cenário cultural, social, político, financeiro, econômico, tecnológico e legal.

Como entrada dessa etapa, estão todas as informações relevantes sobre a organização para a definição do contexto da gestão de riscos, que têm influência direta no gerenciamento de serviços de TI, SI e QoS.

Os contextos interno e externo envolvem as especificações dos critérios básicos necessários para o processo de gestão de riscos; a definição do escopo e dos limites desse processo e o estabelecimento de uma organização responsável pelo processo. Essas especificações e definições compõem a saída dessa etapa, que atuará como entrada da seguinte.

- ANÁLISE/AVALIAÇÃO DE RISCOS E DESEMPENHO – aborda a identificação, quantificação ou descrição qualitativa dos riscos, que são priorizados em função dos critérios de avaliação e dos objetivos da organização. Esta etapa consiste nas atividades de identificação, análise e avaliação de riscos, por meio da identificação do valor dos ativos de informação, das ameaças e vulnerabilidades existentes (ou que poderiam existir). Também, identifica os controles existentes e seus efeitos, determina as consequências e, por fim, prioriza os riscos, ordenando-os de acordo com os critérios de avaliação de riscos estabelecidos na definição do contexto. A saída dessa etapa é formada por uma lista de riscos priorizada de acordo com os critérios de avaliação de riscos, cenários com suas consequências, além de todos os requisitos e controles aplicáveis.

- TRATAMENTO DO RISCO E DESEMPENHO – selecionam-se os controles para modificar, reter, compartilhar ou evitar os riscos, e definir o plano de tratamento do risco, com seus prazos de execução. Os riscos são tratados mediante ordens prioritárias, a fim de implementar as recomendações e decisões. Essas quatro opções disponíveis são selecionadas de acordo com os resultados da etapa anterior, com o custo previsto para implementação de uma ou mais opções escolhidas e com os benefícios esperados. A eficácia do tratamento do risco envolve um processo cíclico para:

  - Avaliar um tratamento do risco;
  - Decidir se os níveis de risco residual são aceitáveis;
  - Gerar um novo tratamento do risco, se os níveis de risco não forem aceitáveis;

- Avaliar a eficácia do tratamento.

Como saída dessa etapa, é fornecido o plano de tratamento do risco e os riscos residuais, sujeitos à aceitação por parte da alta gestão.

- ACEITAÇÃO DO RISCO E DESEMPENHO – decide-se a aceitação dos riscos, formalmente, indicando os responsáveis pela decisão. A saída dessa etapa entrega uma lista de riscos aceitos com as justificativas devidas para os que não foram aprovados pela alta gestão.

- COMUNICAÇÃO DO RISCO E DESEMPENHO – compartilham-se com as partes interessadas, todas as informações sobre os riscos aceitos, seus possíveis impactos e como deve ser realizada a gestão desses riscos. As informações podem incluir a existência, natureza, forma, probabilidade, severidade, tratamento e resultado. Essas informações e o entendimento sobre as atividades de gestão de riscos determina a saída dessa etapa.

- MONITORAMENTO E ANÁLISE CRÍTICA DOS FATORES DE RISCO E DESEMPENHO – desenvolve-se um monitoramento e uma análise crítica sobre os riscos e seus fatores (valores dos ativos, impactos, ameaças, vulnerabilidades e probabilidade de ocorrência), com a intenção de controlar e identificar, tempestivamente, eventuais mudanças no contexto da organização. Os riscos e seus fatores não são estáticos e as mudanças podem ocorrer sem qualquer indicação. Para manter uma visão geral dos riscos é necessário o monitoramento constante, assim como o alinhamento contínuo com os objetivos de negócio da organização e com os critérios para a aceitação do risco da gestão de riscos. Esse alinhamento afeta claramente o gerenciamento de serviços de TI, SI e QoS, e é a saída final do processo principal do modelo.

Em conclusão, o processo de gestão de riscos analisa os possíveis acontecimentos e suas consequências, antes de definir o que será feito e quando será

feito, com o propósito de reduzir os riscos a um nível aceitável. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011b).

A gestão proativa de problemas proporciona uma importante visão sobre os recursos de TI, porque permite analisar as tendências de capacidade, disponibilidade e incidentes recorrentes. Esse processo possibilita antecipar o planejamento das ações de melhorias apropriadas e avaliar se os problemas estão realmente sendo examinados de maneira adequada. Com essa estratégia, torna-se viável alcançar ganhos operacionais e reverter o tempo obtido na redução de carga de trabalho, para solucionar incidentes repetitivos. Portanto, obtém-se um aumento de produtividade e redução de custos para o negócio. Ainda assim, para que essa estratégia conquiste resultados, faz-se necessário um acompanhamento detalhado do processo, pois requer a identificação das causas raiz. Esse modelo de trabalho pode acabar perdendo força, porque com ele é consumido um tempo maior de investigação, contrapondo-se à forte pressão da alta administração para que as causas e soluções de contorno sejam identificadas rapidamente. Essa pressão pode ocasionar respostas ineficazes, retrabalho e aumento dos custos. (CHIARI, 2013).

Por intermédio de monitoramento, análise e tomada de decisões é possível ter uma postura proativa, procurando evitar eventos que gerem instabilidade ou indisponibilidade do ambiente tecnológico. Os alertas de monitoramento informam o incidente sucedido em tempo real, com a especificação do período, uma possível recorrência, e se existe alguma correlação com outra ocorrência. Por conseguinte, torna-se mais factível atender o nível de disponibilidade e capacidade exigidos, atuando de forma rápida e eficiente, com qualidade nas manutenções preventivas e corretivas. Igualmente importante é ter à disposição uma previsão para identificar investimentos a serem realizados, levando-se em consideração a complexidade e criticidade de todo um ambiente, que suporta as mais diversas operações da organização. Com este diagnóstico em mãos, é possível criar um plano de disponibilidade para os serviços críticos, permitindo à alta gestão projetar e decidir qual a disponibilidade exigida e qual o investimento necessário para alcançar esse nível de serviço, o que afeta diretamente os orçamentos da TI.

As empresas deveriam basear suas decisões e seus investimentos em uma estratégia, que equilibre a demanda prevista e a análise do nível dos riscos identificados, sem deixar de considerar a prioridade do negócio, o custo versus o benefício e suas capacidades. Os investimentos podem ser associados da seguinte maneira (TRAUTLEIN; DE LOËS, 2016):

- *Run the Business* (RTB): investimentos realizados para apenas manter a empresa funcionando. Baixo risco. Exemplo: Momentos de crise;
- *Grow the Business* (GTB): investimentos com o propósito de aumentar o valor do negócio. Médio risco;
- *Transform the Business* (TTB): investimentos com a finalidade de transformar o modelo de negócio. Alto risco.

Dessa forma, o modelo proposto permite mitigar os riscos provocados pelos incidentes, por intermédio do monitoramento do ambiente tecnológico, realizando a coleta e identificação dos dados em tempo real, com foco na detecção proativa. Consequentemente, a análise e a resolução de incidentes transcorrem de forma mais ágil e com maior qualidade.

No capítulo subsequente serão detalhados o ambiente no qual foi realizada a experimentação do modelo apresentado e o processo que motivou o seu desenvolvimento.

4 AMBIENTE DE EXPERIMENTAÇÃO

Os quesitos que uma empresa deve cumprir para viabilizar a aplicação do modelo proposto são: possuir o ambiente tecnológico monitorado, dispor de uma central de atendimento como o ponto único de contato para seus usuários e instaurar o GSTI, aplicando as melhores práticas de SI, QoS e da biblioteca ITIL.

A validação do modelo deu-se em uma empresa do segmento da construção pesada, com, aproximadamente, cinquenta obras de médio a longo prazo (entre 2 e 7 anos de duração), em todas as regiões do território nacional e em outros países da América do Sul, América Central e África. Essas obras, em sua maioria, estão estabelecidas em localidades com oferta deficitária de produtos e serviços de TI e telecomunicações. Nesse cenário, a relevância do modelo aumenta, pois tem o objetivo de mitigar os riscos de segurança e desempenho, que são prejudiciais ao negócio.

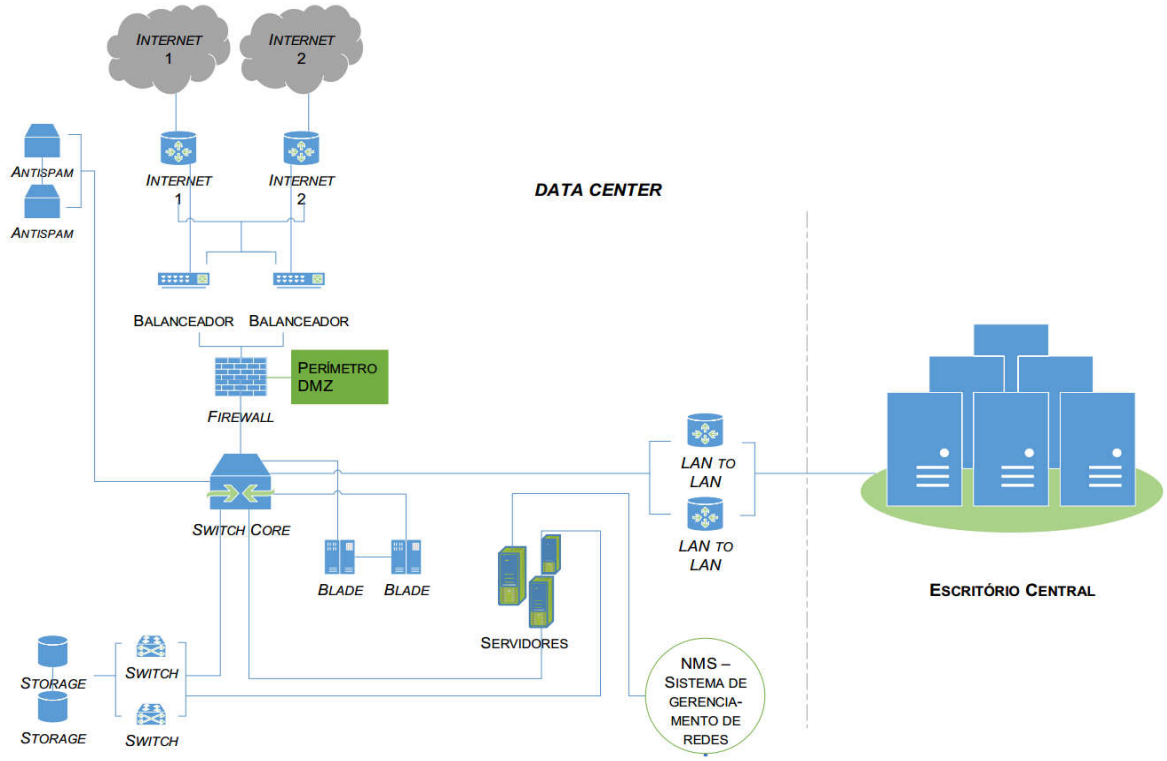
O modelo retrata uma metodologia de gerenciamento de redes de telecomunicações, que utiliza as melhores práticas de ITIL para coordenar ações corretivas sobre os eventos de SI e QoS. Essas ações são realizadas a partir de alertas de monitoramento e registros de ocorrências, com o objetivo de evitar consequências negativas sobre os processos críticos da organização. A lentidão no processamento de um fechamento contábil, a impossibilidade de envio de um relatório financeiro de acompanhamento de resultados e a incapacidade para detectar a causa raiz desses tipos de incidentes são exemplos de ocorrências que prejudicam o negócio e a imagem da área de TI, responsável direta pelo correto funcionamento dos sistemas corporativos. O funcionamento desse modelo torna-se viável a partir da utilização de ferramentas de *service desk* e monitoramento, caracterizadas a seguir.

As ferramentas vieram para facilitar a consecução do objetivo proposto, que é trazer agilidade e qualidade na gestão dos serviços. O *service desk* é uma unidade funcional composta por uma equipe dedicada, responsável por uma variedade de atividades relacionadas aos serviços suportados pela área de TI e utilizados por todas as áreas de negócio. Um *service desk* é disponibilizado por um provedor de serviços, que pode ser interno (a própria TI) ou externo (empresa terceirizada), por meio de um

catálogo de serviços e uma interface via telefone, web, ou notificações automáticas geradas por eventos de sistemas, serviços ou infraestrutura. Apesar da resistência cultural, o *service desk* deve ser o ponto único de contato para os usuários solicitarem suporte às suas demandas, sejam elas incidentes, problemas, requisições ou simples dúvidas. Do mesmo modo, também pode ser a interface para outras atividades, como a comunicação de uma manutenção ou de novos serviços liberados no ambiente de produção. Um *service desk* capaz oportuniza benefícios que enriquecem a percepção e a satisfação dos usuários, aprimora a acessibilidade, por meio de um ponto único de contato, proporcionando uma maior qualidade e agilidade no tratamento das solicitações, além de consolidar informações gerenciais significativas para o apoio à tomada de decisão, indicando também como os serviços de TI suportam processos de negócio da empresa. Em suma, o *service desk* é a vitrine da TI para o bem e para o mal, porque um *service desk* efetivo pode equilibrar as deficiências internas da área de TI, que não são visíveis aos usuários, porém, se for ineficiente, manchará a imagem de toda a área, que terá sua competência e utilidade questionadas.

Diante do exposto, o ambiente de experimentação utilizado para validar o modelo é detalhado na Figura 16, na qual é possível verificar as demandas que envolvem a área de TI. O *service desk* é interno, sendo parte da área de TI, e está localizado no Escritório Central. No fluxo da informação, os sistemas corporativos estão hospedados em um *data center.* As obras se comunicam com eles por meio de sua própria conexão à *internet*, enquanto que a comunicação do Escritório Central ocorre mediante ligação direta (*LAN to LAN*). Para garantir a qualidade dos serviços e a segurança das comunicações, existe uma redundância no *data center*, tanto da ligação direta com o Escritório Central, quanto da conexão à *internet*, que é utilizada para comunicação com as obras.

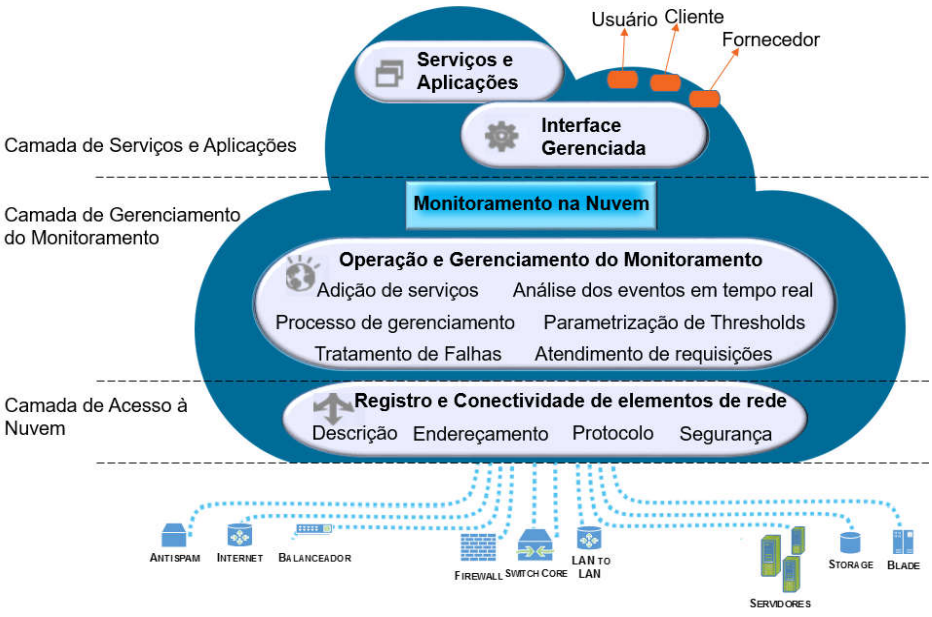
Figura 16. Topologia do ambiente



Fonte: Elaborada pelo autor

Na Figura 17, a seguir, é possível visualizar o NMS - Sistema de Gerenciamento de Redes, mostrado de forma simplificada na Figura 16.

Figura 17. NMS – Sistema de Gerenciamento de Redes



Fonte: Elaborada pelo autor

Pormenorizando o processo que transcorre no NMS - Sistema de Gerenciamento de Redes, são apresentadas suas camadas e as Tabelas 3 e 4, como exemplos de documentos utilizados no modelo apresentado.

Tabela 3. Parametrização de monitoramento

Server	*IP Backup/Gerência*	*Operating System and arquitecture*	*CPU*		*Memory*		*Exceptions*
			Critical	*Major*	*Critical*	*Major*	

Disk Drive			*Up/Down*	*Exceptions*
Unit	*Critical*	*Major*	*Critical*	

Services			*TCP Ports*		*Server / Sistema*	*URLs Monitors*	*Exceptions*
Server	*Service Name*	*Display Name*	*Server*	*Porta*		*URL*	

Fonte: Elaborada pelo autor

Tabela 4. Parametrização para banco de dados

Nome de politica	Descrição	Período	Descrição	Umbral	Objeto
APP-DBSPI-3011	% of current users connected (M011_UserConnectPct)	5m	DBSPI-3011.1	98	
APP-DBSPI-3028	# of databases marked as suspect (M028_SuspectDBCnt)	1h	DBSPI-3028.1	0,5	
APP-DBSPI-3030	Ability to connect to a server (M030_ServerConnect)	5m	DBSPI-3030.1	0,5	
APP-DBSPI-3057	Status of SQL Server service	5m	DBSPI-3057.1	0,5	
APP-DBSPI-3058	Status of SQL Server Agent services	5m	DBSPI-3058.1	0,5	
APP-DBSPI-3081	Replication Agents Status (M081_RepnAgentsStatus)	5m	DBSPI-3081.1	0,5	
APP-DBSPI-3218	% database space used (M218_DBSpaceUsedPct)	1h	DBSPI-3218.1	90	
APP-DBSPI-3230	Ability to connect to a database (M230_DBConnect)	15m	DBSPI-3230.1	0,5	
APP-DBSPI-3234	# of hours since last database transaciton log backup. (M3234_Trar	1d	DBSPI-3234.1	720	
APP-DBSPI-3277	Report on all failed & cancelled jobs (M3277_CompletedJobs)	5m	L3 Jobs		[L3|I3]*
APP-DBSPI-3278	% space used per filegroup and database (M278_FileGrpUsedSpac	15m	DBSPI-3278.1.	95	
Configuração da mensagem					
Criticidade	**Texto da mensagem**				
Critical	% of current users connected (<$VALUE>%) too high (>=<$THRESHOLD>%) for <$OPTION(dbserv)>. [Policy:				
Major	% of current users connected (<$VALUE>%) too high (>=<$THRESHOLD>%) for <$OPTION(dbserv)>. [Policy:				
Critical	<$VALUE> databases marked as suspect for <$OPTION(dbserv)>. [Policy: <$NAME>]				
Critical	Cannot connect to MS SQL Server <$OPTION(dbserv)>.				
Critical	Service MS SQL Server service is down				
Critical	Service MS SQL Server Agent service is down				
Major	One or more replication agents failed.				
Critical	% of space used (<$VALUE>%) on virtual device <$OPTION(virtual_device)> too high (>=<$THRESHOLD>%) for				
Major	Database <$OPTION(database_name)> has not been backed up for <$VALUE> hours (>=<$THRESHOLD> hours) for				
Critical	The transaction log for databases <$OPTION(database_name)> has never been backed up for <$OPTION(dbserv)>.				
Major	The transaction log for database <$OPTION(database_name)> has not been backed up for <$VALUE> hours				
Major	Job failed. Job name = <$OPTION(job_name)>, Job id = <$OPTION(job_id)>, run date = <$OPTION(run_date)>,				
Critical	% filegroup space used (<$VALUE>%) for transaction log filegroup in database <$OPTION(database_name)> too high				

Fonte: Elaborada pelo autor

Na camada de Acesso à Nuvem da Figura 17, essas tabelas são utilizadas para identificação dos elementos a serem monitorados pela ferramenta de monitoramento, de acordo com a criticidade do serviço ou processo de negócio suportado. A Tabela 3 indica que esses elementos podem ser políticas, *site*s (URLs),

portas (*TCP Ports*), serviços (*Services*), bancos de dados, servidores, *switches* e demais componentes do ambiente tecnológico. Na Tabela 4, a parametrização dos servidores de banco de dados é realizada por meio de políticas que informam, por exemplo, a situação de um serviço específico ou percentual de usuários conectados, para um determinado período, umbral e criticidade.

Posteriormente, na camada de Gerenciamento do Monitoramento, são parametrizados seus *thresholds* (limites aceitáveis), por meio de definições de processamento (CPU), memória de execução (*Memory*), espaço em disco (*Disk Drive*) e se está comunicando ou não (*Up/Down*) , por exemplo. Essas definições são obtidas por meio de recomendações de fabricantes, utilização dos elementos e conhecimento aprofundado do ambiente. Contudo, são mutantes e devem ser revistos sempre que necessário. Nessa camada, além da parametrização de *thresholds*, também são realizadas as atividades de análise dos eventos, adição de novos serviços, tratamento de falhas e atendimento de requisições, que pode ser uma atuação presencial de um operador do *data center*. Após cada atuação da equipe de TI, decorrente do recebimento de alertas, os *thresholds* devem ser revisados.

Já na camada de Serviços e Aplicações, os registros que alimentam o modelo podem ser realizados de três formas: i) provenientes de alertas enviados pela ferramenta de monitoramento, ii) pela equipe de TI, de uma forma proativa, ou, iii) reativamente, pelo usuário final. Como pontos de falha e melhoria, a primeira opção pode gerar alertas falsos (falso positivo), devido ao mau funcionamento da ferramenta de monitoramento. As duas últimas opções podem significar uma falha na definição do escopo do monitoramento, na definição dos *thresholds* ou da própria ferramenta de monitoramento. Sob outra perspectiva, o registro reativo pode significar também uma ocorrência que não está no catálogo de serviços da TI, como uma falha no serviço de telefonia, por exemplo. De qualquer forma, o registro realizado pelo usuário final é a opção que menos deveria suceder, porque é a que mais dano causa ao negócio e à TI.

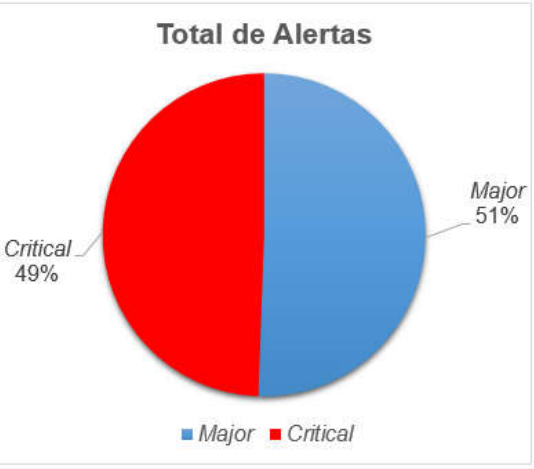
A classificação dos alertas é realizada de acordo com as parametrizações dos *thresholds* e pode ser do tipo menos crítico (*Major*) ou mais crítico (*Critical*). Ambos os tipos de alertas indicam que os *thresholds* foram excedidos, o que dá início ao

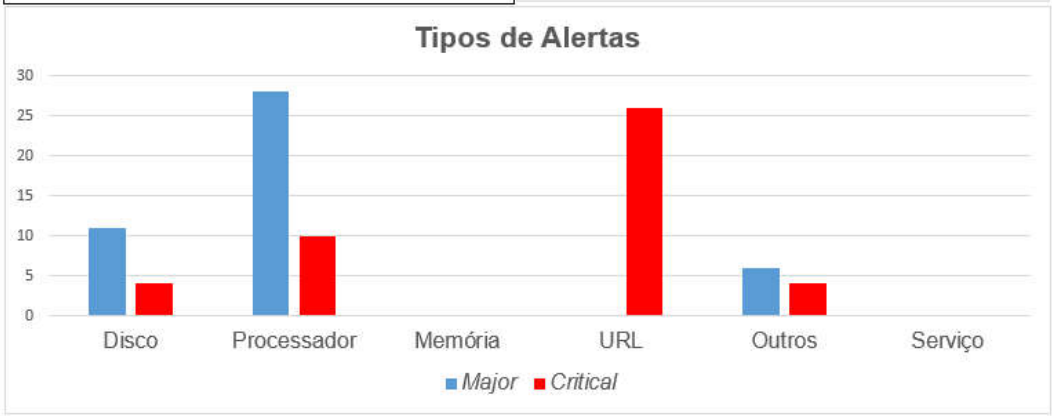
processo de envio de *e-mail* automático para a ferramenta de *service desk*. A ferramenta, também de forma automatizada, registra um incidente ou um incidente maior (incidente de grande impacto, que afeta várias obras e/ou um processo crítico), atribuindo-o ao analista responsável. Em paralelo, a equipe responsável também recebe o *e-mail*, para que possa começar a atuar o quanto antes e mitigar os possíveis impactos. No caso do alerta do tipo *Critical*, também ocorre o acionamento via telefone.

Na Figura 18, é mostrada uma planilha típica de acompanhamento, na qual são gravadas todas as ocorrências. Esse acompanhamento é importante, uma vez que fornece uma visão de possíveis vulnerabilidades e tendências de comportamentos prejudiciais, que podem ser atenuados ou solucionados.

Figura 18. Análise dos alertas

DATA	INICIO	FINAL
	21/10/16	19/02/2017
Alertas por criticidades	***Major***	***Critical***
	45	44
Alertas por criticidades	***Major***	***Critical***
Disco	11	4
Processador	28	10
Memória	0	0
URL	0	26
Outros	6	4
Serviço	0	0
Total	45	44





Fonte: Elaborada pelo autor

Mensalmente, há a necessidade de reiniciar todo o sistema de monitoramento, pois o reenvio de *e-mails* referente aos alertas que não foram tratados pela equipe responsável, deixará de ocorrer. Esse comportamento ocorre, porque há

um entendimento que as devidas ações já foram tomadas, o que pode vir a ser um ponto falho em todo o processo de monitoramento.

Além do monitoramento realizado, os elementos que compõem o ambiente tecnológico estão configurados com o propósito de cumprir os requisitos de QoS e as propriedades de SI. A largura de banda, variação de atraso, perda de pacotes e o atraso são requisitos de QoS. A confidencialidade, integridade e disponibilidade são as propriedades que definem os aspectos de confiabilidade da informação.

4.1 RAO – Relatório de Acompanhamento de Obra

Duas vezes ao mês, em períodos de 4 dias, durante todos os meses do ano, todas as obras devem enviar à área de Orçamentos e Custos, do Escritório Central, o Relatório de Acompanhamento de Obra, RAO, que consiste em um instrumento contábil para seguimento e análises gerenciais das obras ativas. O primeiro dos envios refere-se ao RAO Financeiro e o segundo, ao RAO Econômico. Mediante os resultados desses envios é possível identificar distorções no planejamento e execução dos projetos, por meio dos cálculos previstos e realizados de cada obra. Finalmente, os dados validados e consolidados alimentam o sistema de informação executiva, que apresenta uma visão objetiva e clara para apoiar a alta gestão em tomadas de decisões importantes.

Uma quantidade considerável de obras não cumpre o calendário de entrega e solicita uma postergação do prazo. Esses atrasos, no encerramento e envio dos arquivos, acarretam cobranças de multas internas, além de desgastes entre áreas e até diretorias, pois a área de TI precisa esclarecer e evidenciar a improcedência dos motivos alegados pelas obras para justificar tais atrasos. Esses esclarecimentos nem sempre são incontestáveis, assim como nem sempre é possível obter evidências. Para atender as necessidades do RAO com mais objetividade e transparência, evitando esses desgastes, foi idealizado o modelo apresentado.

As principais atividades que devem ser realizadas para emissão do RAO são apresentadas em seguida. Por motivo de segurança, as atividades não estão detalhadas:

1. Apontamento do avanço físico das tarefas executadas no mês;
2. Custo direto - Atualização do planejamento;
3. Recebimento, impostos, aportes e transferências – Atualização do planejamento;
4. Custo indireto - Atualização do planejamento;
5. Elaboração de lista com todos os contratos ativos;
6. Lançar todas as previsões do relatório enviado pelo setor de medição, com data base do último dia do mês da ocorrência do fato;
7. Lançar os impostos referentes ao recebimento do mês anterior, por meio da rotina Contas a pagar;
8. Lançar todas as medições enviadas pelo setor de medição, com data base do último dia do mês da ocorrência do fato;
9. Cancelar as previsões restantes, conforme orientação do setor de medição, com data base do último dia do mês anterior;
10. Verificar se a conciliação bancária está concluída e integrada. Caso esteja, informar ao planejamento;
11. Avaliar encontro de contas (obras de Consórcio);
12. Verificar aplicações financeiras (obras de Consórcio);
13. Calcular o avanço físico (acompanhamento real da execução do serviço);
14. Fazer uma análise crítica das variações do avanço físico atual em relação ao anterior;
15. Calcular o realizado do RAO financeiro;
16. Emitir o relatório de conferência do realizado do mês base e verificar se os lançamentos estão corretos (valores, classificação/linha do RAO);
17. Calcular o previsto do RAO Financeiro;
18. Emitir o relatório de Contas a Pagar do módulo de contabilidade gerencial (RAO) e conferir se todos os lançamentos foram feitos;
19. Emitir o *Drill down* das linhas do RAO Financeiro e verificar se os lançamentos estão corretos;

20. Fazer uma análise crítica das variações do RAO Financeiro atual em relação ao RAO anterior e ao RAO do PEC;

21. Conferir sempre se o percentual total de encargos sociais está coerente;

22. Calcular o realizado do RAO Econômico (quando a contabilidade estiver “fechada”);

23. Emitir o relatório de conferencia do realizado do mês anterior e verificar se os lançamentos estão corretos (valores e classificação/linha do RAO);

24. Calcular o previsto do RAO Econômico;

25. Emitir o *Drill down* das linhas do RAO Econômico e verificar se os lançamentos estão corretos;

26. Fazer uma análise crítica das variações do RAO Econômico atual em relação ao RAO anterior e ao RAO do PEC;

27. Analisar o RAO Econômico Patrimonial para identificação de distorções em relação ao RAO Econômico de Resultado.

Como o RAO é um processo estrategicamente crucial para a organização, durante o período de sua realização, todas as áreas envolvidas ficam em estado de alerta, para atender qualquer eventualidade que possa dificultar ou impedir sua conclusão. O processamento do RAO é realizado por intermédio de um *Enterprise Resource Planning* (ERP), sistema de gestão empresarial, subdividido em dois sistemas, que, neste caso, são dependentes. O primeiro integra os dados e processos das áreas de engenharia, de orçamento e planejamento, e o segundo integra os dados e processos das demais áreas de negócios, como Controladoria, Tesouraria, Compras, entre outras. É importante salientar que as sessões dos usuários, utilizadas para acessar os dois sistemas necessários para o processamento do RAO, têm a possibilidade de estar configuradas para conectar-se a eles, por meio de redes privadas (VPNs) criptografas. Essa tecnologia melhora a estabilidade, desempenho e segurança das conexões, principalmente contra a perda de pacotes de dados. Sendo assim, se por um lado, a criptografia dos dados afeta o desempenho das comunicações, por outro, a segurança dos dados é reforçada com informações fornecidas pelo sistema QoS. (ALMERHAG *et al*., 2010).

Na Figura 19, observa-se que os principais fluxos de processos do modelo têm influência sobre o funcionamento do RAO.

Figura 19. RAO – Relatório de Acompanhamento de Obra

Fonte: Elaborada pelo autor

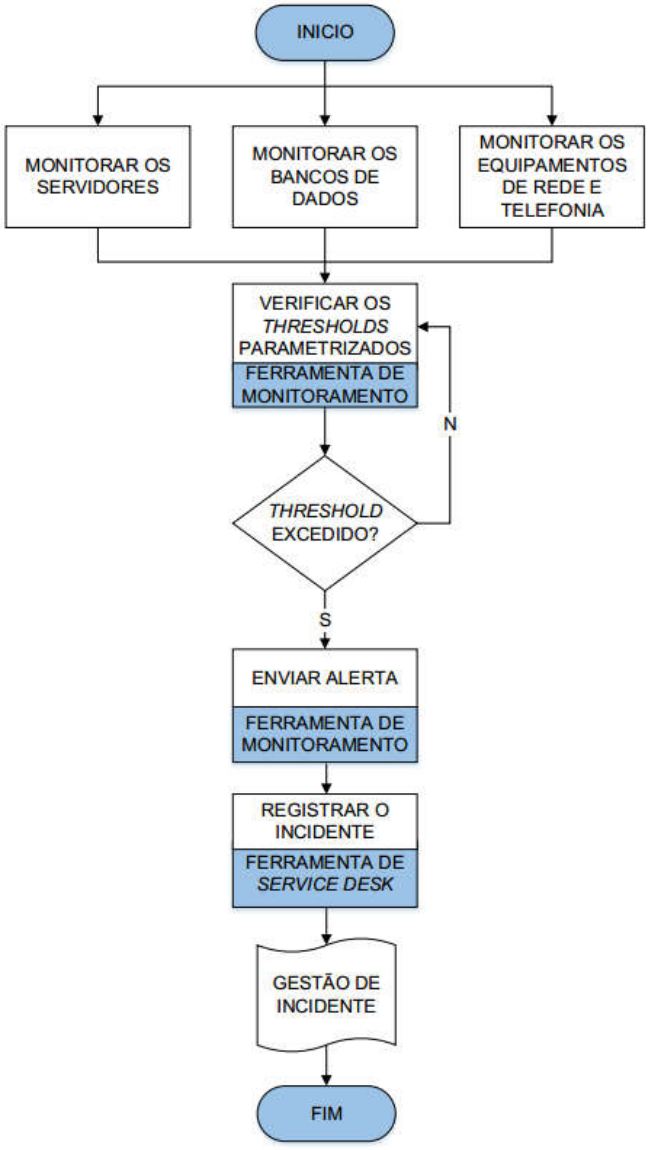
O monitoramento do ambiente tecnológico, o gerenciamento de mudanças e as gestões de incidentes e problemas possuem processos, ocorrem de forma contínua, entre os blocos da Figura 14, referente ao modelo proposto.

Figura 14. Diagrama do modelo proposto

Fonte: Elaborada pelo autor

No primeiro bloco, ocorrem os registros de chamados, por meio dos processos de monitoramento da Figura 20.

Figura 20. Monitoramento de Ambientes

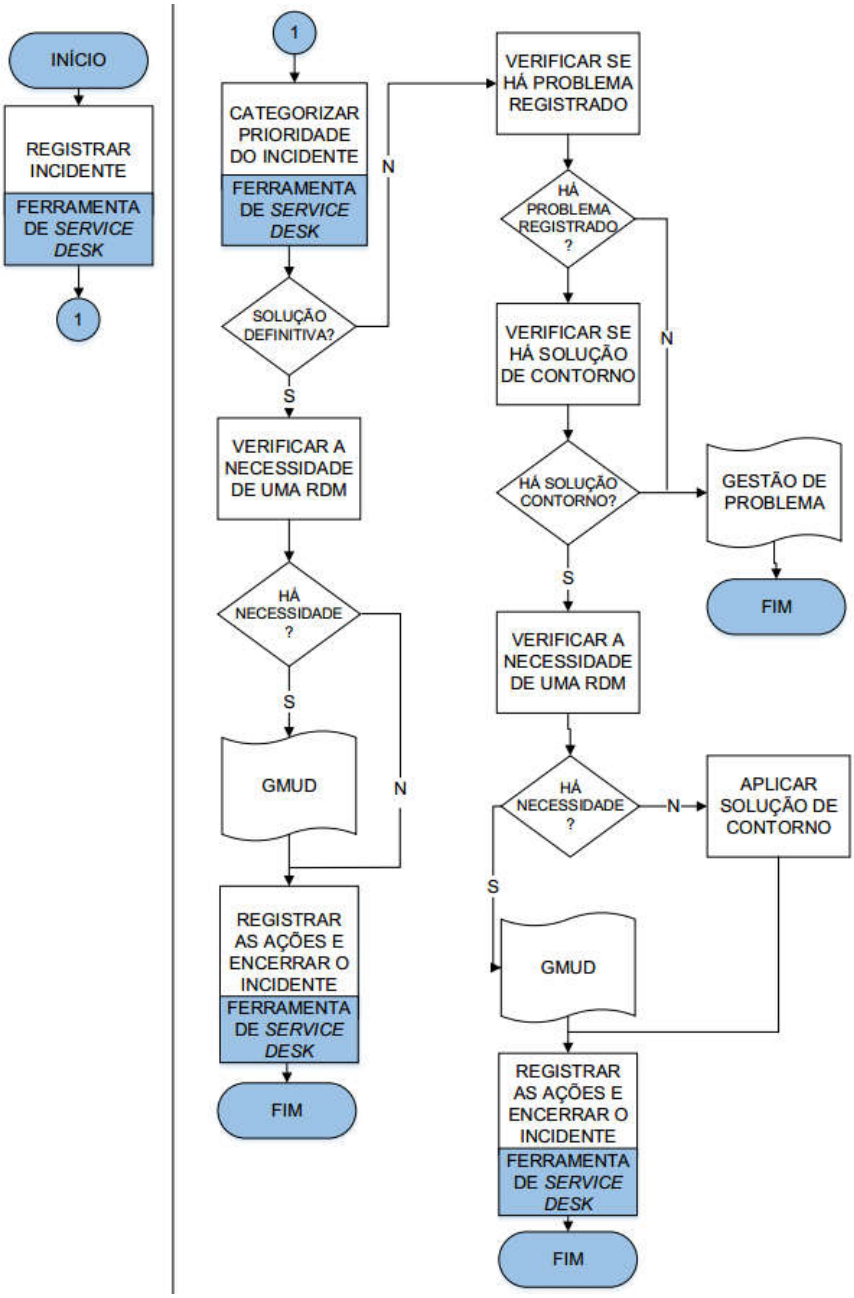


Fonte: Elaborada pelo autor

Essa figura mostra que o ambiente tecnológico é monitorado, de acordo com a parametrização de *thresholds*, dos elementos de rede. A ferramenta de monitoramento, de forma automatizada, envia um alerta, quando é identificado que um *threshold* foi excedido, e a ferramenta de *service desk* realiza o registro de um incidente. A partir desse registro, **já no segundo bloco da Figura 14**, iniciam-se as

análises e tratamentos pertinentes para a resolução desse incidente, seguindo os processos contidos no fluxo de Gestão de Incidentes, da Figura 21.

Figura 21. Gestão de Incidentes

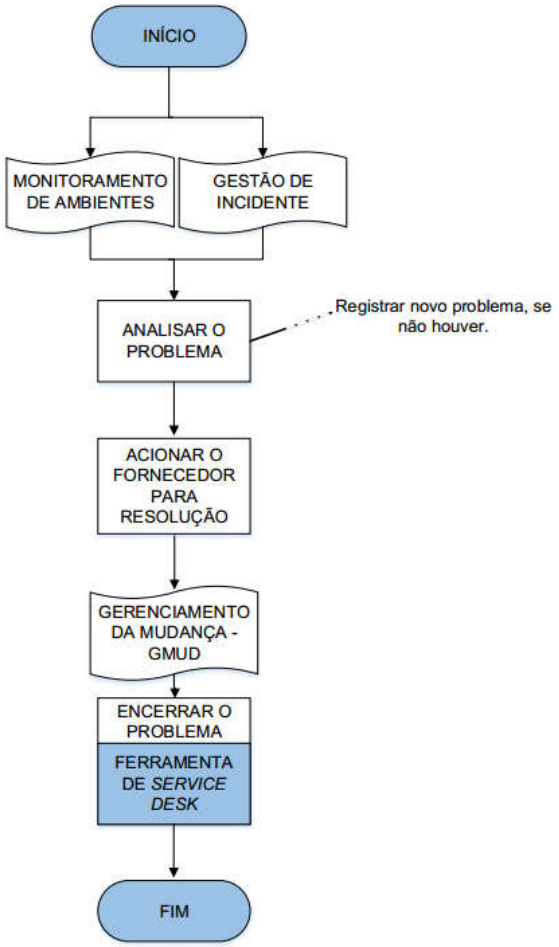


Fonte: Elaborada pelo autor

Nessa figura, de forma resumida, as informações dos alertas enviados são analisadas detalhadamente, para classificar e definir o tipo e a prioridade do incidente. Se for possível encontrar uma solução definitiva ou de contorno, o incidente é tratado e o chamado relacionado é encerrado. O encerramento do chamado ocorre **no terceiro e**

último bloco da Figura 14. Se a solução encontrada não for definitiva (solução de contorno) ou se não for encontrada nenhuma solução, dão-se início as ações necessárias, conforme os processos contidos no fluxo de Gestão de Problemas, da Figura 22. A diferença fundamental entre um incidente e um problema está na possibilidade de identificação da causa raiz (incidente) ou não (problema), da ocorrência.

Figura 22. Gestão de Problemas

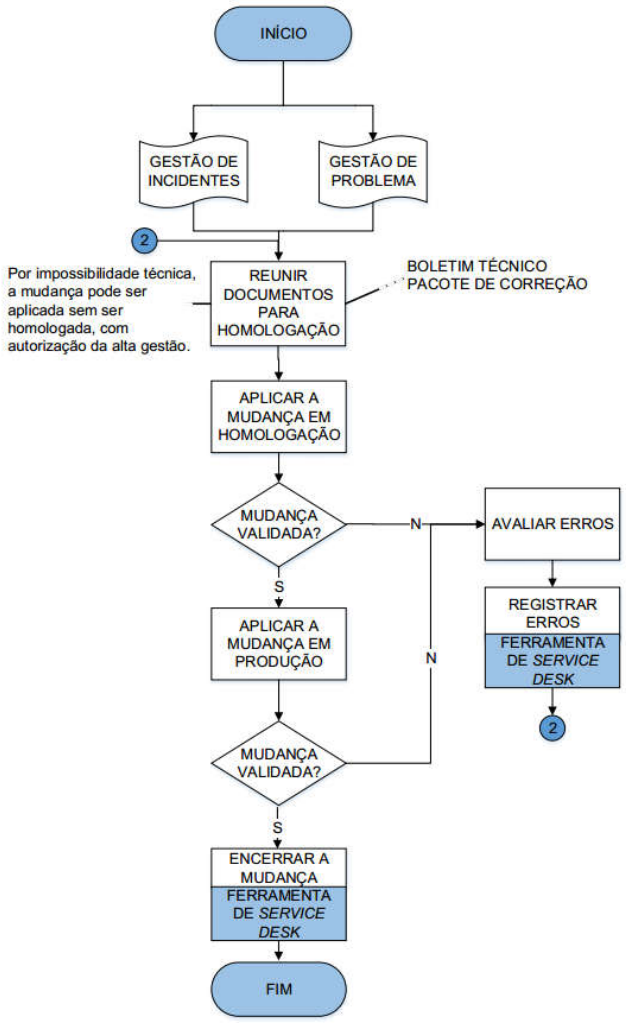


Fonte: Elaborada pelo autor

Nessa figura, após esgotadas as tentativas de resolução, por parte da equipe interna da TI, ocorre o acionamento do fornecedor para que seja identificada a causa raiz da ocorrência e encontrada uma solução para o problema.

A Figura 23 exibe o fluxo responsável pelas mudanças detectadas e inevitáveis, tanto na Figura 21. Gestão de Incidentes quanto na Figura 22. Gestão de Problemas.

Figura 23. Gerenciamento de Mudanças (GMUD)



Fonte: Elaborada pelo autor

Os processos dessa figura definem uma sequência de etapas, nas quais são realizadas as homologações e validações das implementações, para garantir que a entrega tenha qualidade e não afete negativamente o ambiente de produção. Dessa forma, procura-se evitar erros e outras eventualidades.

Durante cada ação tomada, em cada bloco da Figura 14. Diagrama do modelo proposto, os processos dos fluxos apresentados são executados e interagem entre eles, concluindo as fases necessárias até o encerramento do chamado.

No próximo capítulo serão explorados os resultados obtidos e os benefícios decorrentes da aplicação do modelo.

5 RESULTADOS

Neste capítulo, são apresentados e discutidos os resultados obtidos após a implantação do modelo em uma empresa de grande porte, do setor de construção pesada. Para compreender melhor o modelo, é mostrado o seu funcionamento, por meio de um exemplo real.

Mediante os processos executados em cada bloco da Figura 14 (Capítulo 4, página 65), juntamente com a execução dos processos pertinentes aos fluxos citados anteriormente (Capítulo 4, página 65), é possível percorrer esse exemplo, que é detalhado em seguida, por meio de etapas.

Como informado (Capítulo 4, página 65), o sistema de gestão empresarial, ERP, está localizado em um *data center*. As obras efetuam o processamento e envio do RAO, por meio de sua própria rede. A área de Orçamento e Custos, que está no Escritório Central, ratifica e valida esse recebimento mediante uma conexão direta com o *data center*. Um ponto de falha importante desse ERP é a alta sensibilidade à perda de dados, com as seguintes orientações do fabricante:

- *Ping* entre 201 e 320ms -> Risco na integridade da informação;
- *Ping* acima de 320ms -> Risco de perda da comunicação.

Etapa 1, passando pelo bloco 1 da Figura 14. Diagrama do modelo proposto e pela Figura 20. Monitoramento de Ambientes

Por meio dos monitoramentos realizados, um alerta foi enviado pela ferramenta de monitoramento e a ferramenta de *service desk* registrou um incidente. Ambas ações foram processadas de forma automatizada. Esse alerta foi do tipo mais crítico e indicou que o *threshold*, referente ao espaço livre de uma partição do servidor de banco de dados, do ERP, foi excedido.

Etapa 2, passando pelo bloco 2 da Figura 14, pela Figura 21. Gestão de Incidentes e Figura 23. Gerenciamento de Mudanças (GMUD)

A partir desse registro, as informações do alerta enviado foram analisadas e avaliadas, para fim de classificar e definir o tipo e a prioridade do incidente. O

incidente foi classificado como Incidente Maior, pois verificou-se a possibilidade de alto impacto ao negócio, já que podia estar afetando vários processos críticos, de todas as obras e do Escritório Central. Foi definido o contexto da unidade envolvida diretamente, no caso, *data center*. Nessa definição de contexto, o objetivo é obter a maior quantidade de informações úteis sobre o (s) ambiente (s), para que a atuação tenha o máximo de assertividade possível. Foram verificadas as informações sobre a localização, tipos de acesso, perfis de usuário, módulos utilizados, rotinas executadas e ambiente tecnológico, tais como condições de servidores (de aplicação, banco de dados, licenciamento, etc), serviços, *links* (LAN to LAN e *internet*), *firewalls*, antivírus, *backups*, etc. Iniciaram-se as análises e avaliações minuciosas dos riscos e desempenho, e foi realizado o tratamento por meio dos procedimentos apropriados da lista de verificações, para a resolução desse incidente. No entanto, juntamente com o fornecedor, decidiu-se encerrar o incidente, com a aplicação de duas soluções de contorno e registrar um problema, para identificar a causa raiz e encontrar uma solução definitiva. A primeira solução de contorno realizada foi o aumento imediato da partição afetada, pois essa não gerava indisponibilidade sistêmica, por se tratar de um ambiente virtual. A segunda solução de contorno realizada foi a posterior limpeza dessa partição, no primeiro período possível para essa manutenção, pois poderia gerar indisponibilidade sistêmica. Essas mudanças necessárias foram implementadas, seguindo os processos do fluxo de Gerenciamento de Mudanças, da Figura 23, para evitar erros e contingência no ambiente de produção.

Etapa 3, passando pelo bloco 2 da Figura 14, pela Figura 22. Gestão de Problemas e Figura 23. Gerenciamento de Mudanças (GMUD)

Após esgotadas as tentativas para uma resolução definitiva do incidente, ocorreu a mobilização do fornecedor para resolução do problema. O mesmo identificou a causa raiz e disponibilizou a correção da rotina, que motivou esse comportamento atípico do banco de dados do ERP. Os processos, da Figura 23, foram empregados para homologar e validar a correção, e o problema foi solucionado.

Etapa 4, passando pelo bloco 3 da Figura 14, pela Figura 21. Gestão de Incidentes e Figura 22. Gestão de Problemas

Os encerramentos dos chamados relativos ao incidente e problema ocorreu no terceiro e último bloco da Figura 14. Durante cada ação tomada, em cada bloco da Figura 14, os processos dos fluxos apresentados são executados e interagem entre eles, concluindo as fases necessárias até o encerramento do chamado.

Esse exemplo sucedeu antes de um período inicial de RAO, sendo possível a resolução do problema a tempo, de forma proativa, evitando desgastes desnecessários. Da mesma maneira, viabilizou-se a tomada de decisões importantes, com uma maior eficiência na entrega de informações estratégicas.

As informações provenientes do RAO são fulcrais e devem ser irrefutáveis. No entanto, o RAO é um processo complexo, com diversas possibilidades de cálculos, verificações e análises, que provocam dúvidas e falhas de procedimentos dos usuários. Com relação aos sistemas, há ocorrências referentes aos erros, parametrizações e configurações. Quanto à infraestrutura, há ocorrências que afetam o funcionamento do ambiente tecnológico, ocasionando lentidão, instabilidade ou indisponibilidade das comunicações e dos sistemas corporativos. Por outro lado, na Tabela 5, são apresentadas algumas das principais vulnerabilidades identificadas com o auxílio da norma NBR ISO / IEC 27005, responsáveis pela maioria dos erros que ocorrem durante o período de entrega do RAO. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011b).

Tabela 5. Principais vulnerabilidades aplicáveis adaptado

Tipo	Exemplo de Vulnerabilidades	Exemplo de ameaças
Software	Falhas conhecidas no software	Abuso de direitos
Software	Não execução do *logout*, ao se deixar uma estação de trabalho desassistida	Abuso de direitos
Software	Inexistência de uma trilha de auditoria. Repercute no desempenho	Abuso de direitos
Software	Atribuição errônea de direitos de acesso	Abuso de direitos
Software	Interface de usuário complicada	Erro durante o uso
Software	Configuração de parâmetros incorreta	Erro durante o uso
Rede	Tráfego sensível desprotegido	Escuta não autorizada
Rede	Ponto único de falha. Nesse caso, ausência de equipamento de segurança sugerido nas obras (plataforma de segurança com antivírus, *firewall*, IPS, VPN e filtro web)	Falha do equipamento de telecomunicação

Rede	Gerenciamento de rede inadequado (roteamento)	Saturação do sistema de informação
RH	Treinamento insuficiente, tanto sistêmico quanto de SI	Erro durante o uso
Organização	Inexistência de procedimento de monitoramento das instalações de processamento de informações	Abuso de direitos

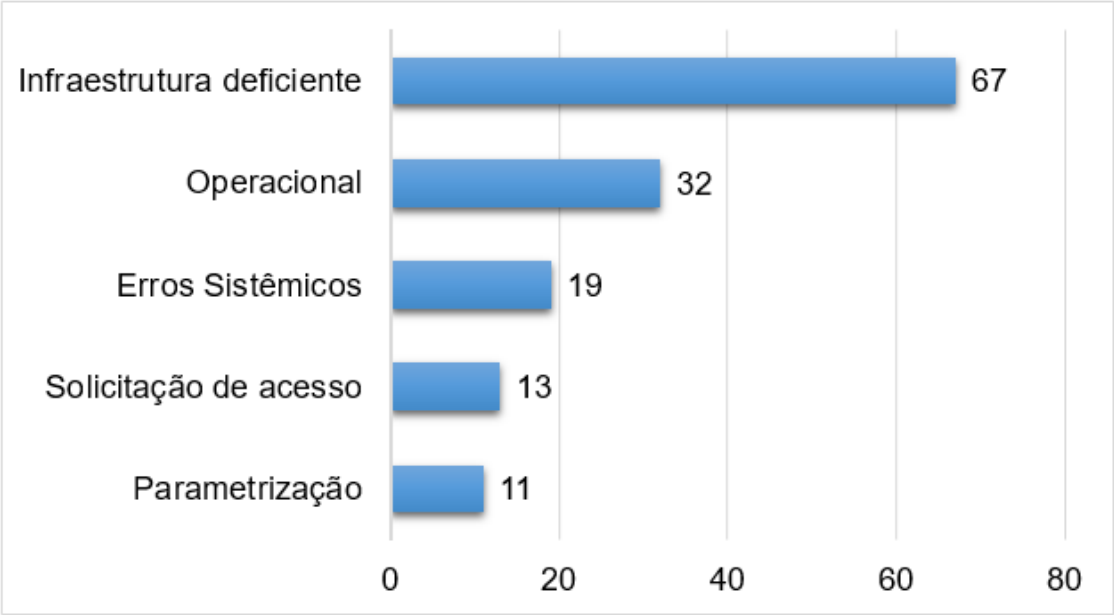
Fonte: Elaborado pelo autor

Perante o exposto, e baseando-se também nas informações sobre vulnerabilidades da Tabela 5, as ocorrências foram divididas em cinco tipos, que são de Infraestrutura deficiente, Operacional, Erros sistêmicos, Solicitação de acesso e Parametrização.

Para validar o modelo foi realizado um levantamento com uma amostra de ocorrências relacionadas ao RAO, desde 01/01/2015 até 09/05/2016, e realizada uma comparação com o período compreendido entre 10/05/2016 e 18/01/2017, a partir do qual foram implementadas as mudanças propostas pelo modelo. Uma vez que os períodos são diferentes, levou-se em consideração a quantidade de obras. No entanto, durante o período da amostragem, não houve variação.

As 142 ocorrências registradas entre 01/01/2015 e 18/01/2017 estão classificadas na Figura 24:

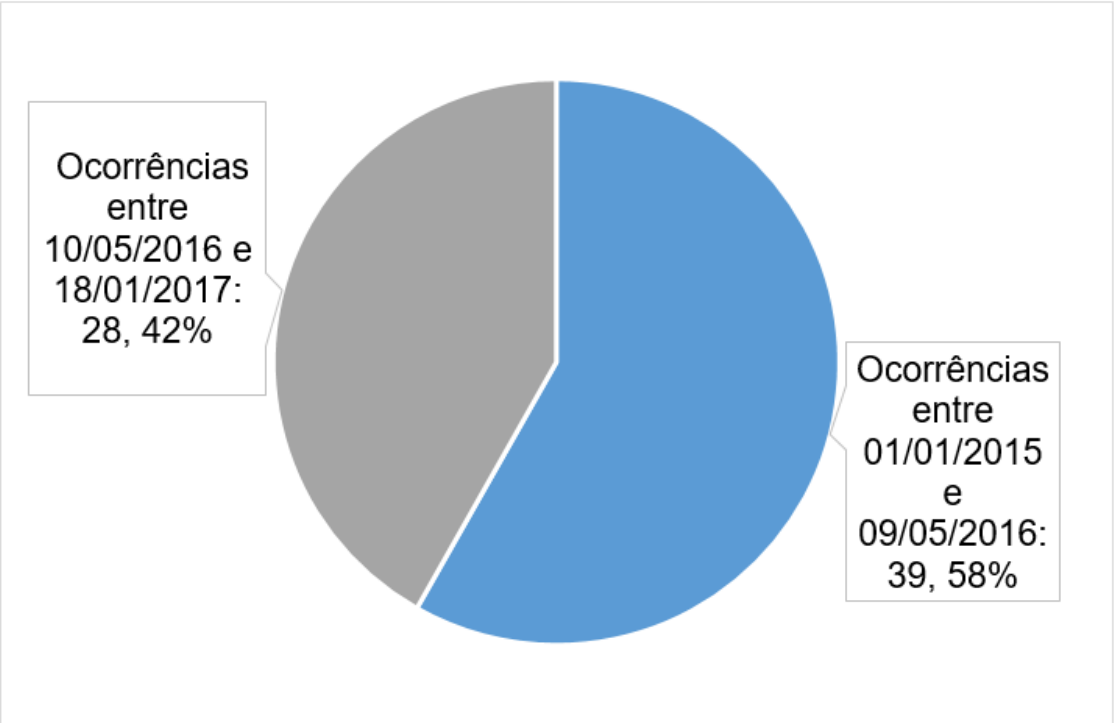
Figura 24. Total de ocorrências entre 01/01/2015 e 18/01/2017



Fonte: Elaborado pelo autor

No período entre 01/01/2015 e 18/01/2017, 67 (47%) ocorrências estiveram diretamente ligadas a incidentes de SI e QoS, considerando as ocorrências do tipo Infraestrutura deficiente. Essas ocorrências estão relacionadas ao desempenho insuficiente ou erros sistêmicos provocados por uma infraestrutura deficiente das obras ou do *data center*. Dessas 67 ocorrências, 39 (58%) foram anteriores à implementação do modelo e 28 (42%) foram posteriores, como apresentado na Figura 25:

Figura 25. Ocorrências relacionadas à infraestrutura deficiente



Fonte: Elaborado pelo autor

As melhorias realizadas na infraestrutura foram:

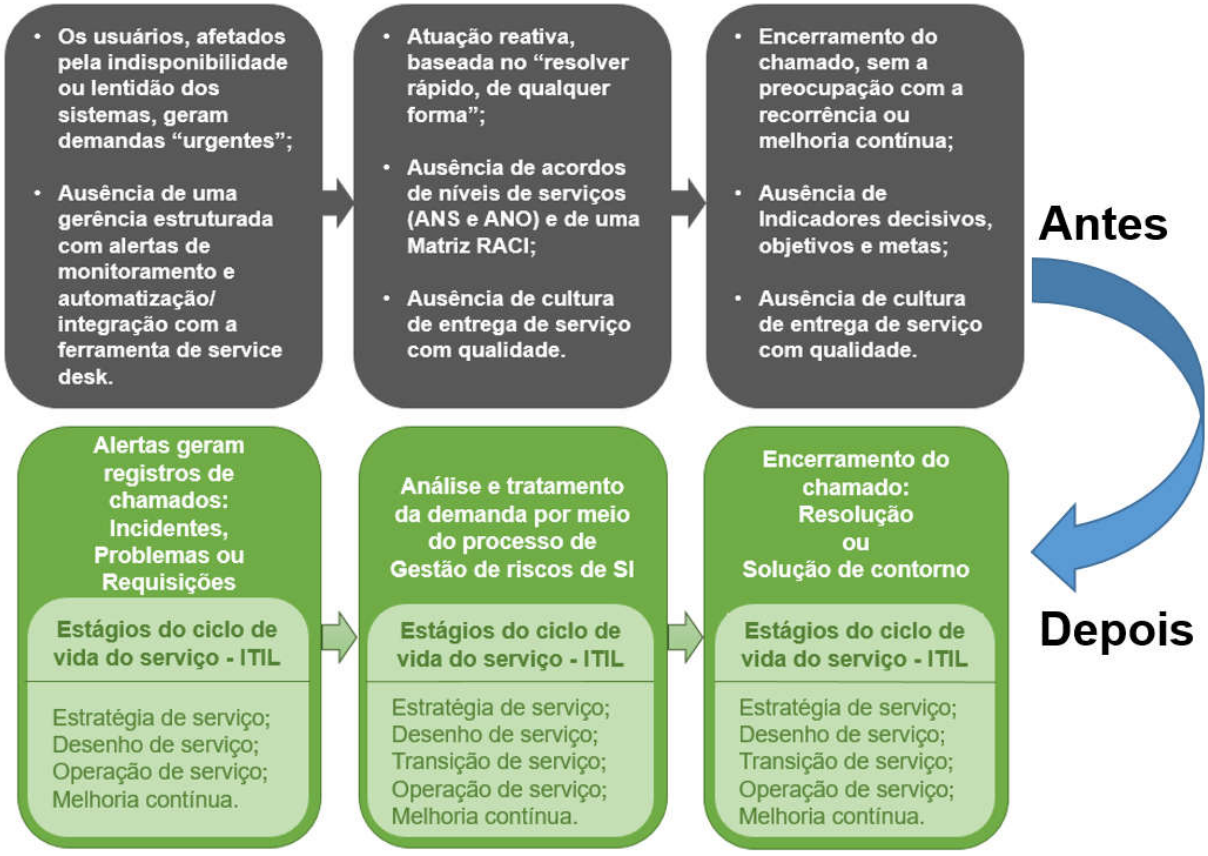
- **Mudança de link internet** – de acordo com a capacidade necessária, em função da análise da quantidade de usuários pela largura de banda;
- **Padronização da configuração de acesso aos sistemas corporativos, via VPN criptografada** – torna as comunicações mais seguras e estáveis;
- **Exigência da utilização da solução de segurança (UTM)** – evitando a lentidão no acesso à internet e vulnerabilidades na rede interna;

- **Revisão dos dispositivos de TI e do ambiente tecnológico.**

Portanto, é possível afirmar que houve uma mitigação das ocorrências desse tipo, em razão da aplicação do modelo apresentado, com importantes benefícios para todas as áreas de negócios envolvidas. Esses benefícios foram constatados por meio da estabilização de serviços críticos e redução da quantidade de incidentes, possibilitando maior agilidade no fornecimento de informações estratégicas para a tomada de decisão. Do mesmo modo, houve benefícios relacionados à melhor compreensão, por parte da TI, de procedimentos operacionais dos usuários, estrategicamente críticos, que contribuem para um conhecimento mais específico do funcionamento técnico dos sistemas.

A Figura 26 compara a forma de atuação da área de TI, antes e depois da aplicação do modelo, destacando as principais diferenças percebidas.

Figura 26. Antes e Depois do Modelo.



Fonte: Elaborada pelo autor

Antes, a ferramenta de *service desk* era pouco desenvolvida e automatizada, baseada em e-mails e processos manuais. A atuação da TI era totalmente reativa e não havia monitoramento nem alertas, com definições coesas dos *thresholds*. Também não existia uma definição de acordos de níveis de serviços (SLA) e nem de responsabilidades (matriz RACI). Os indicadores eram insuficientes e não refletiam as necessidades da área de TI e do negócio, pois não respondiam os questionamentos da alta gestão.

Depois, instaurou-se uma gerência estruturada para planejar, executar, monitorar e buscar uma melhoria contínua. Essa mudança cultural, baseada no GSTI, causou um impacto direto na forma de atuação da TI. Como resultado, ocorreu a otimização e integração da ferramenta de *service desk* com a ferramenta de monitoramento. A ferramenta de *service desk* foi parametrizada com os acordos de níveis de serviços e com a matriz de responsabilidade, enquanto que a ferramenta de monitoramento foi configurada com *thresholds* em conformidade com a realidade do ambiente tecnológico.

No próximo capítulo serão apresentadas as conclusões deste trabalho e as tendências que podem afetar as operações de TI, além de algumas possibilidades de trabalho futuro.

6 CONCLUSÃO E TRABALHOS FUTUROS

Neste trabalho, propôs-se um modelo a para o gerenciamento de redes de telecomunicações, fundamentada em ITIL, e apoiada na segurança da informação e na qualidade dos serviços. Este modelo foi validado mediante um processo de negócio real, em uma grande empresa de construção pesada. No Capítulo 5, além dos resultados gerais, descreveu-se o tratamento completo de um incidente. Apresentaram-se as análises, avaliações e tratamentos necessários para solução do incidente. No entanto, em função dos recursos disponíveis no momento, encerrou-se o incidente com soluções paliativas. Desta forma, registrou-se, então, um problema e pressionou-se o fornecedor, que identificou a causa raiz e enviou a correção necessária. Com isso, resolveu-se o problema e encerrou-se o chamado.

Antes da implementação dessa proposta, os incidentes de SI e QoS, considerando as ocorrências do tipo Infraestrutura deficiente, representavam 58% (39) do total de incidentes do escopo da área de TI. Após a mudança realizada, houve uma diminuição para 42% (28), o que significa uma redução de, aproximadamente, 16% desse tipo de ocorrência. Esse resultado viabiliza comunicações mais seguras e estáveis, provendo melhor desempenho e maior produtividade.

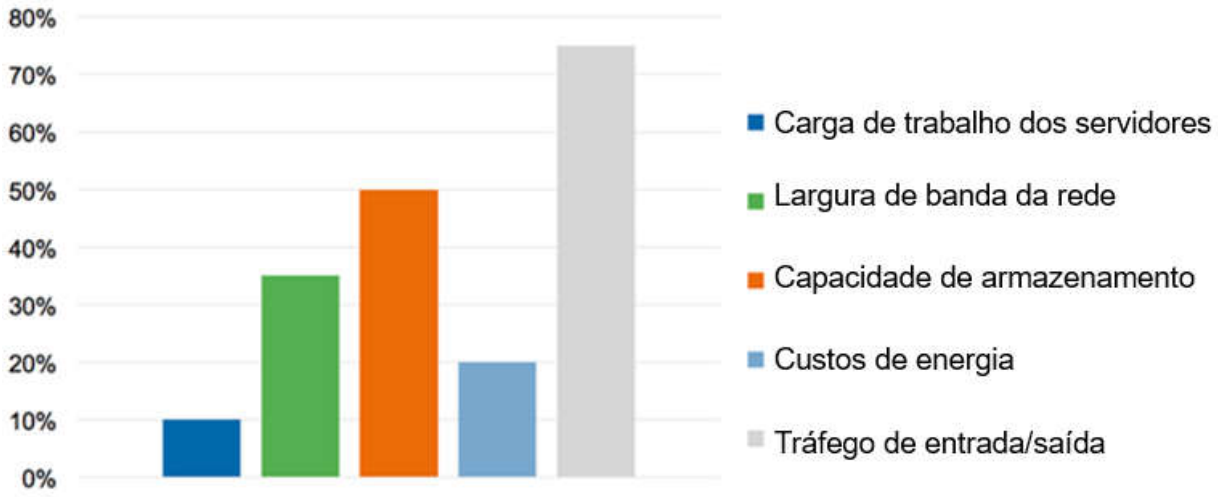
É importante ressaltar que, ao longo de 2016, houve uma mudança profunda na arquitetura do ambiente tecnológico, decorrente da transferência de grande parte da infraestrutura para um *data center* externo. Essa mudança provocou uma série de manutenções necessárias, que afetou os usuários, inclusive nos períodos do RAO. No entanto, todas as ocorrências relacionadas à infraestrutura deficiente foram contabilizadas e classificadas como tal, o que significa que o resultado poderia ter sido ainda melhor. Por outro lado, devido à diminuição da quantidade de obras, por causa da crise política e econômica que atinge o país desde 2014, houve também uma redução significativa no registro de ocorrências.

A sequência deste trabalho prevê expandir o estudo para as obras, que carecem do conhecimento e apoio técnico. O objetivo será, por meio dos resultados obtidos, obter o patrocínio da alta gestão para viabilizar a padronização da infraestrutura de TI e administração do ambiente tecnológico, em todas as obras.

Desse modo, procura-se mitigar os incidentes, facilitar o diagnóstico e agilizar a resolução das ocorrências, além de proporcionar um ambiente propício para o desempenho das atividades, visando o aumento da produtividade. Também como trabalho futuro, serão analisadas as possibilidades de utilização de mais processos do ciclo de vida do serviço da ITIL, controles das normas de SI e implementação de políticas de *QoS*, para o desenvolvimento de uma melhor qualidade de experiência do usuário, QoE (*Quality of Experience*). Ademais, buscar-se-á a adequação às principais tendências tecnológicas relacionadas com o enfoque do modelo proposto. Na pesquisa da *Gartner, As 10 tendências emergentes e seus impactos na sua operação de TI*, são apresentadas as tendências que trarão impactos diretos na forma como a área de TI fornece serviços ao negócio, até 2021. (CAPPUCCIO, 2016). Na sequência, são detalhadas essas que são mais relevantes para o modelo:

- **Demanda sem interrupções** – remete à exigência de alta disponibilidade, considerando o aumento de demanda de carga de trabalho dos servidores, largura de banda de rede, capacidade de armazenamento, custos de energia e tráfego de entrada e saída de dados, conforme indicado pelo crescimento anual de demandas (Figura 27).

Figura 27. Crescimento anual de demandas adaptado



Fonte: Cappuccio (2016)

Na Figura 28, a seguir, é possível observar o aumento previsto para os próximos cinco anos, contabilizando a quantidade de novos servidores, dados e conexões.

Figura 28. Aumento previsto da demanda adaptado

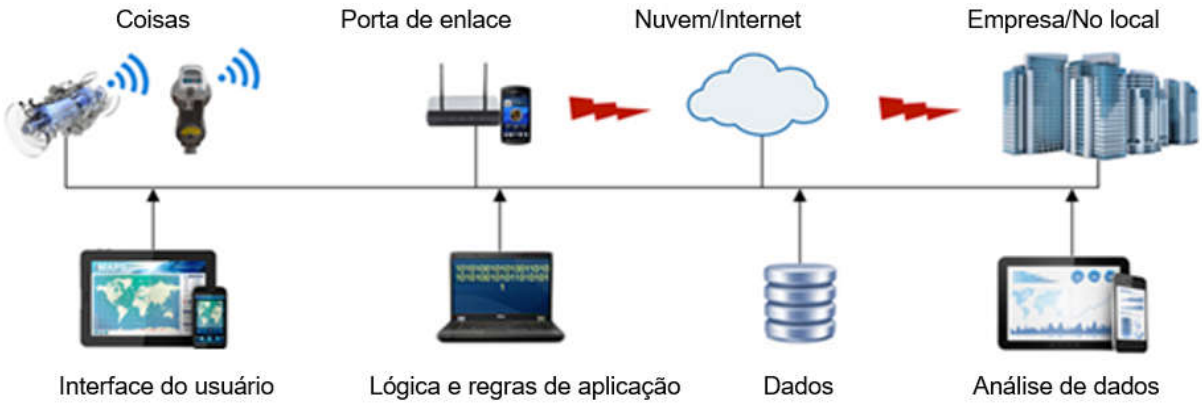
Escala	Infraestrutura do Centro de Dados		
	Servidores (Unid.)	Armazenamento (TB)	Networking
Mudança Social			
Ascensão da Classe Média			
Envelhecimento da População	2012: 9,7 bilhões	18,4 milhões	0,1 milhão
Novas Tecnologias	2015: 10,6 bilhões	37,8 milhões	2,2 milhões
Digitalização	2019: 11,9 bilhões	89,2 milhões	8,4 milhões
Hiperconectividade			

Fonte: Cappuccio (2016)

A ascensão da classe média, o envelhecimento da população, as novas tecnologias e a mudança de comportamento social são os principais motivadores desse incremento. Como consequência desse crescimento vertical, o foco estará voltado, cada vez mais, para o planejamento, gerenciamento de recursos e capacidade, com atenção especial para a energia, refrigeração e espaço de armazenamento.

- **Computação de borda** – a experiência do usuário final, por meio de pequenos dispositivos, serviços dependentes de latência, *sites* remotos, IoT, *Big Data* e aplicações baseadas em geolocalização, como exibido na Figura 29, continuará sendo de responsabilidade da TI. Por esse motivo, essa experiência deve estar orientada com base na necessidade e viabilidade quanto aos serviços híbridos em nuvem, que evoluem rapidamente.

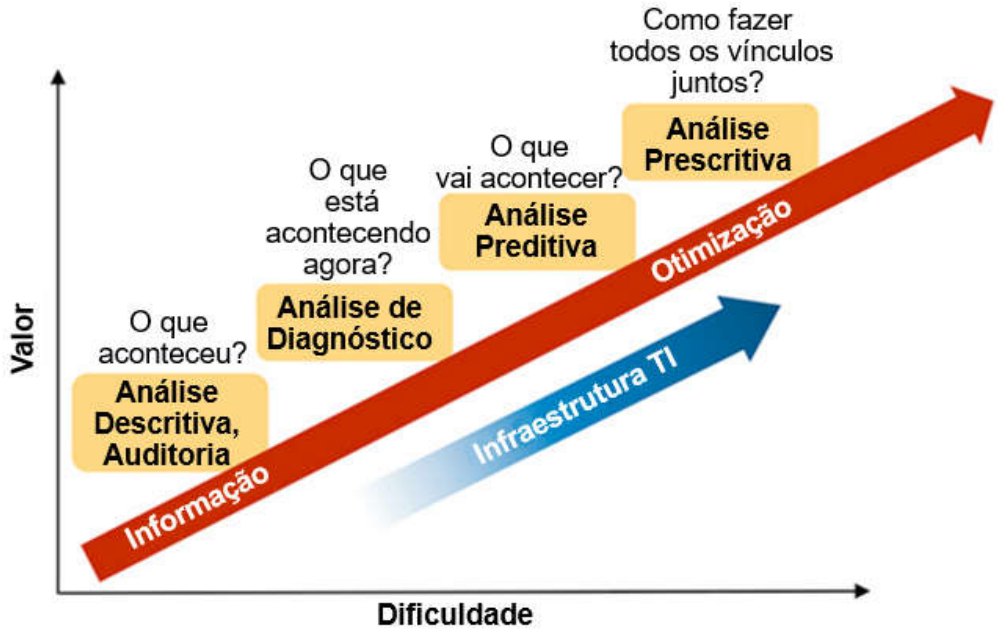
Figura 29. Computação de borda adaptado



Fonte: Cappuccio (2016)

- **Gerenciamento global do centro de dados** – contempla o centro de dados em toda a parte e a capacidade para gerenciá-lo. Considera-se, por exemplo, o gerenciamento remoto de ativos, as conexões e suas dependências, o planejamento de recursos e os relatórios e *dashboards*. Na Figura 30, observa-se uma busca pela otimização do ambiente tecnológico e dos serviços entregues, à medida que os diferentes tipos de análises são realizadas, de forma sucessiva.

Figura 30. Gerenciamento global do centro de dados adaptado



Fonte: Cappuccio (2016)

A Análise Descritiva permite saber o que aconteceu no passado. A Análise de Diagnóstico comunica o acontecimento presente. A Análise Preditiva possibilita a projeção de tendências, mediante a identificação da probabilidade de resultados futuros, com base em dados históricos. Por fim, a Análise Prescritiva sugere como se deve agir. Em contrapartida, a complexidade do gerenciamento aumenta ao passo que as análises evoluem.

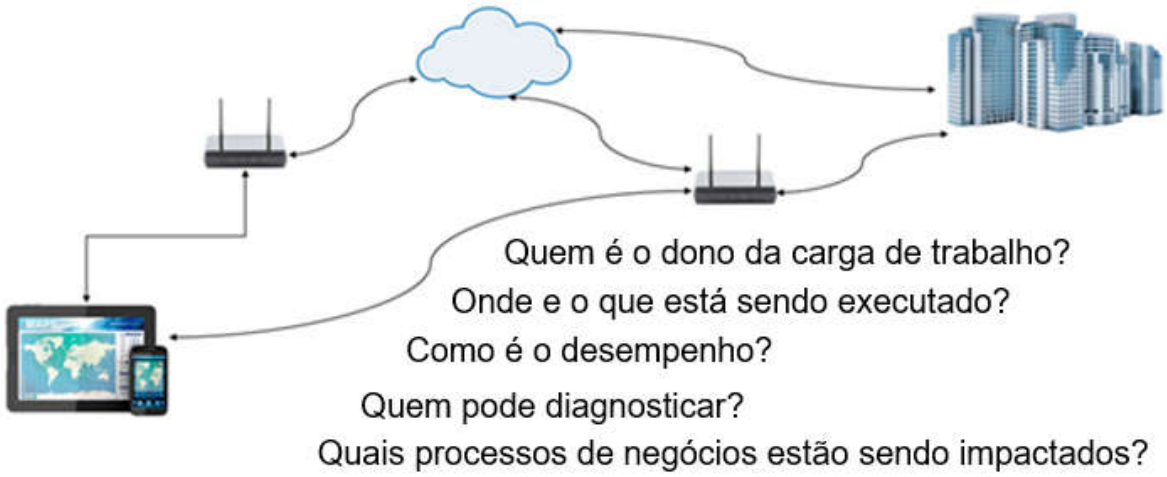
- **Gerenciamento de infraestrutura composta** – refere-se ao gerenciamento de uma infraestrutura, cujos recursos tecnológicos físicos, como servidores, *storage* e demais elementos de rede, são administrados como serviços e agrupados logicamente, como máquinas virtuais. Na Figura 31 são mostradas as informações do ambiente necessárias para realizar o gerenciamento.

Figura 31. Gerenciamento de infraestrutura composta adaptado

Fonte: Cappuccio (2016)

Na Figura 32, são exibidos questionamentos, cujas respostas são informações igualmente necessárias para o gerenciamento da infraestrutura composta. Novas tecnologias, como DevOps e SDN, estão empregando e destacando essa tendência.

Figura 32. Gerenciamento dos serviços de TI adaptado



Fonte: Cappuccio (2016)

A menos que a TI entenda como essas tendências estão surgindo e quais serão (ou já são) os efeitos em cascata sobre suas operações, os impactos na estratégia, no planejamento estratégico e nas operações poderão ser significativos.

7 REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO / IEC 20000: Tecnologia da Informação – Gestão de Serviços – Parte 1: Requisitos do sistema de gestão de serviços**. Rio de Janeiro, 2011a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO / IEC 27005: Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação**. Rio de Janeiro, 2011b.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO / IEC 27001: Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos**. Rio de Janeiro, 2013a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO / IEC 27002: Tecnologia da Informação – Técnicas de segurança – Código de Prática para controles de segurança da informação**. Rio de Janeiro, 2013b.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO / IEC 27032: Tecnologia da Informação – Técnicas de segurança – Diretrizes para segurança cibernética**. Rio de Janeiro, 2015.

ALBUQUERQUE, Eduardo. **QoS – Qualidade de Serviço em Redes de Computadores**. Campus Elsevier, 2013.

ALMERHAG, I. A. et al. ***Network security for QoS routing metrics.*** In: COMPUTER AND COMMUNICATION ENGINEERING (ICCCE), 2010. International Conference on. IEEE, 2010. p. 1-6.

AXELOS. Available from: <https://www.axelos.com/>. Cited: 31 mar. 2017.

BAARS, Hans et al. ***Foundations of information security based on ISO27001 and ISO27002.*** 3. ed. Van Haren, 2015.

BOURNE, Vanson. ***IT Trust CURVE.*** EMC, 2013. Disponível em: <http://brazil.emc.com/collateral/other/emc-trust-curve-es.pdf>. Acesso em: 31 mar. 2017.

CAPPUCCIO, David J. ***Top 10 Emerging Trends and Their Impacts On Your IT Operation.*** GARTNER, 2016. Available from: <https://www.gartner.com/technology/media-products/reprints/microsoft/1-2YJLGOW/index.html>. Cited: 31 mar. 2017.

CHIARI, Renê Abrileri. **ITIL® na Prática – Gerenciando Problemas de Infraestrutura e Serviços de TI – Uma abordagem prática para o planejamento, implementação, operação e melhoria contínua.** [s.n.], 2013.

CHIARI, Renê Abrileri. **ITSM na Prática – O caviar de 5 anos de postagens.** [s.n.], 2014.

COOPERS, Price Waterhouse. ***The Global State of Information Security Survey 2016.*** 2016.

FRICKÉ, Martin. ***The knowledge pyramid: a critique of the DIKW hierarchy. Journal of information science,*** v. 35, n. 2, p. 131-142, 2009.

HATTINGH, Christina; SZIGETI, Tim. ***End-to-end QoS Network Design: Quality of Service in LANs, WANs and VPNs.*** USA: CiscoPress, 2004. p. 44.

IEC. Available from: <http://www.iec.ch>. Cited: 31 mar. 2017.

ISACA. Available from: <http://www.isaca.org>. Cited: 03 may. 2017.

ITU. Available from: <https://www.itu.int/rec/T-REC-E.800-200809-I>. Cited: 03 may. 2017.

ISO. Available from: <http://www.iso.org/iso/home.html/>. Cited: 31 mar. 2017.

IETF. Available from: < https://www.ietf.org/>. Cited: 31 mar. 2017.

KEEN, Peter G. W. ***Information technology and the management difference: a fusion map. IBM Systems Journal,*** v. 32, n. 1, p. 17-39, 1993.

KUNAS, Michael. ***Implementing Service Quality based on ISO/IEC 20000: A management guide.*** IT Governance Publishing, 2012.

KUROSE, James F.; ROSS, Keith W.; ZUCCHI, Wagner Luiz. **Redes de Computadores e a Internet: uma abordagem top-down.** Pearson, 2010.

LAURINDO, Fernando José Barbin et al. **O papel da tecnologia da informação (TI) na estratégia das organizações. Gestão & Produção,** v. 8, n. 2, p. 160-179, 2001.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. **Gerenciamento de serviços de TI na prática: uma abordagem com base na ITIL**. Novatec Editora, 2007.

NÜRNBERGER, A.; WENZEL, Constanze. ***Wisdom-the blurry top of human cognition in the DIKW-model?*.** In: Proceedings of the EUSFLAT conference, Aix-Les-Bains, France. 2011. p. 584-591.

PINHEIRO, Lena Vania Ribeiro. **Informação: esse obscuro objeto da ciência da informação. Revista Morpheus-Estudos Interdisciplinares em Memória Social**, v. 3, n. 4, 2004.

PROOF. ***in|secu.re – information security curation report 2016.*** PROOF, 2016. Disponível em: <http://insights.proof.com.br/insecure>. Acesso em: 31 mar. 2017.

ROMETTY. Ginni, CEO, IBM. ***New Ways of Thinking about Enterprise Security.*** In: IBM Security Summit, 2015. IBM, 2015.

SAKARINDR, P. et al. ***Security-enhanced quality of service (SQoS) design and architecture.*** In: IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication, 2005. IEEE, 2005. p. 129-132.

SELM, Leo Van. ***ISO/IEC 2000 – An Introduction.*** Van Haren, 2008.

SILVA, Marcelo Gaspar Rodrigues; GOMEZ, Thierry Albert M. Pedroso; MIRANDA, Zailton Cardoso de. **TI: mudar e inovar: resolvendo conflitos com ITIL v3: aplicado a um estudo de caso**. Brasília: Senac DF, 2010.

SZIGETI, Tim et al. ***End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks.*** Cisco Press, 2013.

TRAUTLEIN, Barbara A.; DE LOËS, Christian. ***Build Change Intelligence to Bridge the Gap between Strategy and Execution.*** 2016.

WETHERALL, J.; TANENBAUM, A. S. **Redes de Computadores**. 5ª edição. Pearson, 2011.

APÊNDICE A – Lista de verificações de requisitos de QoS e controles de SI

Na Tabela 6 estão presentes os requisitos de QoS e os controles de SI, listados na norma NBR ISO / IEC27002, aplicáveis ao processo exposto na seção VI. Ambiente de Experimentação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b).

Tabela 6. Lista de verificações de requisitos de QoS e controles de SI

QoS – *Quality of Service*
Requisitos monitorados, que impactam na qualidade do serviço:
Largura de banda ou vazão
Atraso, retardo ou latência
Variação de atraso ou flutuação do tempo de transmissão (*jitter*)
Perda de pacotes de dados
A.5 Política de segurança
A.5.1 Orientação da direção para segurança da informação
Objetivos: Prover orientação da direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes**.**
Tratamento: Controle inicial e essencial para implantação do SGSI, patrocinado pela alta gestão.
A.6 Organização da segurança da informação
A.6.1 Organização interna
Objetivos: Estabelecer uma estrutura de gerenciamento, para iniciar e controlar a implementação e operação da segurança da informação, na organização**.**
Tratamento: Controle inicial e essencial para implantação do SGSI, patrocinado pela alta gestão.
A.6.2 Dispositivos móveis e trabalho remoto
Objetivos: Garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis.
Tratamento: Ativar o acesso via VPN criptografada, normatizar a obrigatoriedade de aquisição/configuração da solução de segurança (UTM), por parte das obras, e verificar o acesso via LAN to LAN (para o Escritório Central).
A.9 Controle de acesso
A.9.1 Requisitos do negócio para controle de acesso
Objetivos: Limitar o acesso a informação e aos recursos de processamento da informação.

Tratamento: Revisar os grupos e perfis de acesso para evitar um perfil conflitivo ou a lentidão de acesso e de processamento das rotinas devido a um perfil abrangente (Empresas e filiais desnecessárias).
A.10 Criptografia
Objetivos: Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.
Tratamento: Ativar o acesso via VPN criptografada (SSL 256 Bits) e normatizar a obrigatoriedade de aquisição/configuração da solução de segurança (UTM), (até AES 256), por parte das obras.
A.11 Segurança física e do ambiente
A.11.2 Equipamentos
Objetivos: Impedir o comprometimento de ativos e interrupção das operações da organização. Manutenção correta para assegurar sua disponibilidade e integridade permanente.
Tratamento: Revisar equipamentos de TI afetados e o ambiente ao qual pertencem.
A.12 Segurança nas operações
A.12.1 Responsabilidades e procedimentos operacionais
Objetivos: Garantir a operação segura e correta dos recursos de processamento da informação para preservar a disponibilidade e integridade das informações.
Tratamento: Normatizar um calendário de treinamentos sobre o ERP, para não permitir procedimentos que causem indisponibilidade, baixa performance ou falta de integridade dos dados. Como exemplos: CTRL + ALT + DEL durante processamento, várias sessões abertas para o mesmo usuário, execução em modo MDI do ERP, seleção de período extenso para processamento, habilitar auditoria do ERP, etc.
A.12.2 Proteção contra *malware*
Objetivos: Assegurar que as informações e os recursos de processamento da informação estão protegidos contra *malware*.
Tratamento: Gerenciar a solução de antivírus e atuar sobre os incidentes de segurança da informação, apresentados por meio de relatórios de monitoramento.
A.12.7 Considerações quanto à auditoria de sistemas de informação
Objetivos: Minimizar o impacto das atividades de auditoria nos sistemas de informação.
Tratamento: Planejar as atividades seguindo o fluxo de processo de mudanças existente, com o objetivo de não impactar nos processos.
A.13 Segurança nas comunicações
A.13.1 Controle de redes

Objetivos: Assegurar a proteção das informações em redes e dos recursos de processamento da informação que os apoiam.
Tratamento: Idem tratamento A.6.2 e monitorar e controlar as ferramentas de SI: balanceador, filtro de conteúdo, *antispam*, VPN, *storage* e *firewall*.
A.13.2 Transferência de informação
Objetivos: Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas.
Tratamento: Idem tratamento A.6.2 e monitorar e controlar as ferramentas de SI: balanceador, filtro de conteúdo, *antispam*, VPN, *storage* e *firewall*.
A.14 Aquisição, desenvolvimento e manutenção de sistemas
A.14.2 Segurança em processos de desenvolvimento e de suporte
Objetivos: Garantir que a segurança da informação está projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação.
Tratamento: Realizar a melhoria contínua e auditoria do fluxo de processo de mudanças existente (análise, homologação e validação), que controla também os fontes do sistema enviados pelo fornecedor.
A.15 Relacionamento na cadeia de suprimento
Objetivos: Mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização.
Tratamento: Controlar o acesso dos fornecedores. O acesso indevido pode afetar diretamente o desempenho das comunicações e a segurança das informações.
A.16 Gestão de incidentes de segurança da informação
Objetivos: Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de SI.
Tratamento: Utilizar o fluxo de processo de mudanças existente para tratar incidentes de segurança da informação.
A.18 Conformidade
Objetivos: Evitar a violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à SI.
Tratamento: Atualizar as normas, procedimentos operacionais e processos e procedimentos internos da TI, de acordo com as recomendações da auditoria e lições aprendidas dos registros dos chamados.

Fonte: Elaborado pelo autor