South American Development Society Journal

Vol.: 04, | Nº.: 12 | **Ano:** 2018 | **ISSN:** 2446-5763 | **DOI:** 10.24325/issn.2446-5763.v4i12p230-242
Data de Submissão: 04/11/2018 | **Data de Publicação:** 19/12/2018

VISÃO HOLISTICA DA GESTÃO DE ATIVOS NA TECNOLOGIA DA INFORMAÇÃO

Renata Farragoni Rodrigues da Silva Sodré - Instituto Federal de Educação, Ciência e Tecnologia de São Paulo - Câmpus Bragança Paulista
rfarragoni@gmailcom

Prof. Dr. Orlando Leonardo Berenguel - Instituto Federal de Educação, Ciência e Tecnologia de São Paulo - Câmpus Bragança Paulista
oberenguel@ifsp.edu.br

Resumo

Buscando contribuir com o tema de gestão de ativos em departamentos de Tecnologia da Informação (TI), este artigo objetivou meios de como a implementação da gestão de ativos de TI contribui para a organização alcançar a eficiência operacional para a redução da responsabilidade legal e extensão de danos causados pelo desajuste em seu funcionamento. Através de pesquisas bibliográficas em periódicos e publicações relevantes, este assunto pouco tem sido abordado, do ponto de vista acadêmico, mesmo que exista o entendimento intrínseco de que ativos de TI devam ser controlados no cenário industrial e tecnológico para salvaguardarem o ambiente operacional de operações fraudulentas de qualquer natureza. Tais medidas preventivas, são alcançadas, quando os processos da operação do negócio tenham atrelados à eles padrões (difundidos no mercado) e Normas Internacionais que viabilizem a gestão de serviços de TI, a fim de, aplicar reformas para arrumar o que não está certo e incentivar a organização rumo à modernização administrativa.

Tais abordagens, de gestão e gerenciamento, podem ser alcançadas com o auxílio da implementação do conjunto de Normas ABNT ISO/IEC 55000 e ISO/IEC 19770 que permitirão conhecer e registrar onde e para quem, os ativos de hardware e software de TI estão oferecendo serviço e assim controlar a extensão do dano e as responsabilizações legais dos envolvidos.

Palavras-chave: gestão e ativos; ABNT ISO/IEC 55000; ISO/IEC 19770; tecnologia da informação; responsabilidade legal.

Abstract

Seeking to contribute to the topic of asset management in Information Technology (IT) departments, this article aimed at how the implementation of IT asset management contributes to the organization to achieve operational efficiency for reducing legal liability and extension of damages caused by the mismatch in its operation. Through bibliographic research in relevant journals and publications, this subject has been rarely approached from the academic point of view even though there is an intrinsic understanding that IT assets should be controlled in the industrial and technological setting to safeguard the operating environment from fraudulent operations of any nature. Such preventive measures are achieved when the processes of business operation have attached to them standards (disseminated in the market) and International Standards that enable the management of IT services, in order to implement reforms to correct what is not right and encourage the organization towards administrative modernization. Such management and administration approaches can be achieved with the implementation of the set of ISO / IEC 55000 and ISO / IEC 19770 standards that will allow to know and record where and for whom IT hardware and software assets are offering service and thus control the extent of demage and legal liability of those involved.

Keyword: asset management; ABNT ISO / IEC 55000; ISO / IEC 19770; information technology; legal responsibility.

Introdução

Nos últimos anos, tem-se presenciado ao redor do mundo, notícias sobre crimes econômicos com base em subornos, fraudes, subversão de fundos de investimentos, extorsão e abuso de confiança societária (Higor. J. et.al., 2015). Na contramão disto, algumas organizações, que possuem grandes investimentos em processos informatizados procuram reduzir suas perdas financeiras através de controles internos e sistemas transparentes aos seus colaboradores; que se inteligentemente ordenados e gerenciados, estes controles e sistemas, podem vir a mitigar a progressão de fraudes e sua detecção tão breve quanto for possível. Para Gesteira, sócio da KPMG, (KPMG, 2016) um controle interno é deficiente quando mal planejado e quando não é seguido pelos empregados deixando portas abertas para fraudes, e somente uma avaliação minuciosa do risco de fraude consegue demonstrar onde estão as lacunas.

À estas factuais notícias, devemos considerar que por trás da prática destes grandes crimes, os envolvidos na ilicitude, fizeram uso de ferramentas tecnológicas relacionadas aos produtos de software (programas), hardware (dispositivos físicos) e a rede de computadores em que eles estavam conectados. À estes crimes se aplica o termo "crime cibernético", que nesta reflexão, foram somados aos fatos, a existência do envolvimento direto e indireto de funcionários (ou colaboradores) vinculados a empresa. Uma vez que eles tendo o conhecimento sobre a forma de operação do sistema da "Organização" e as suas brechas técnicas nas práticas flexíveis de trabalho, para eles a fraude se tornou muito mais fácil e tentadora para se ganhar vantagens facilmente; funcionários (ou colaboradores) atuam como peças-chave na idealização de golpes e operações fraudulentas (Higor. J. et.al., 2015).

Neste cenário devastador, existem aqueles indivíduos que podem ser afetados pelas atividades desempenhadas pela organização ou seja, prejudica a reputação das empresas, custa milhões e arruína vidas (KPMG, 2016), uma vez que, as operações do negócio podem ocasionar transformações "negativas" na sociedade, mudanças climáticas regionais ou globais e, entre outros, a ampliação da desigualdade social (IBGC, 2018).

Neste sentido, tendo em vista a probabilidade de ocorrência de deformações na sociedade, o ordenamento jurídico da região onde a organização tem as suas opera-

ções regulará as responsabilidades dos seus dirigentes. No Brasil, a pessoa jurídica da empresa e, ou, sua pessoa física, terá responsabilidade cível e, ou, criminal pelos atos ilícitos dos seus colaboradores, quando estes fizerem o mau uso do recurso tecnológico que a organização disponibilizar à eles como ferramenta de trabalho para ser utilizada dentro ou fora do ambiente corporativo (Higor. J. et.al., 2015).

No tocante de tais responsabilizações, medidas de prevenção de incidentes e mitigação de ameaças, que impactem negativamente a operação da organização (se implementadas e geridas eficaz e eficientemente) permitem que a organização obtenha redução da sua responsabilidade legal e a extensão do dano (Higor. J. et.al., 2015). Tais medidas preventivas são alcançadas, quando os processos da operação do negócio tenham atrelados à eles padrões (difundidos no mercado) e Normas Internacionais que viabilizem a gestão de serviços de Tecnologia da Informação (TI), a fim de, aplicar reformas para arrumar o que não está certo e incentivar a organização rumo à modernização administrativa.

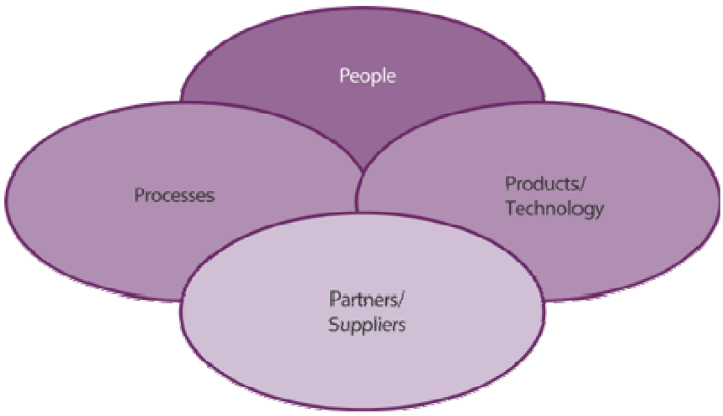
Neste sentido, o departamento de TI, junto de seus administradores terão a capacidade de oferecer suporte à administração, mitigação de ameaças e resolução de incidentes de forma mais rápida e eficiente quando eles conhecerem todo o seu parque tecnológico para aplicar uma gestão e gerenciamento efetivo dos ativos em todo o seu ciclo de vida (desde a aquisição até o descarte). Tais abordagens, de gestão e gerenciamento, podem ser alcançadas com o auxílio da implementação das Normas ISO/IEC 55001 (ABNT ISO 55000, 2014) e ISO/IEC 19770-1 (ISO/IEC 19770-1, 2017) que permitirão conhecer e registrar onde e para quem, os ativos de hardware e software de TI estão oferecendo serviço e assim controlar a extensão do dano e as responsabilizações legais dos envolvidos.

Assim, o objetivo dessa pesquisa é revisar a literatura acerca dos conceitos, normas e processos de gerenciamento de ativos abrangidos pelo conjunto de Normas ISO/IEC 55000: Gestão de ativos (ABNT ISO 55000, 2014) e ISO/IEC 19770-1 Information technology -- Software asset management (ISO/IEC 19770-1, 2017).

1. GESTÃO DE ATIVOS DE TI

Um ambiente de TI é composto por seus empregados e colaboradores, por seus processos organizacionais, por seus serviços e recursos tecnológicos, e por seus fornecedores e fabricantes envolvidos na entrega dos seus serviços. Os chamados 4P's: People, Products, Processes and Partners (definidos pela IT Infrastructure Library - ITIL) (Taylor, 2011).

Figura 1 – 4 P's da biblioteca ItIL



Fonte: ItIL v3: Service Design

Onde o objetivo destes 4P's é fornecer uma abordagem holística que garanta não apenas as características de finalidade e de uso (ou funcionalidades), mas também os aspectos de garantia vinculados aos níveis de serviço acordados com os clientes.

Vista esta breve abordagem de quais recursos devem ser considerados em uma operação dos serviços de TI, se torna crucial que todos os envolvidos entendam que não se olha apenas para a solução em si, mas também para tudo o mais que gerenciará a qualidade do serviço de forma à atender: as necessidades do negócio; da equipe de TI durante o desenvolvendo e gerenciando o serviço; e dos usuários do serviço.

Desta forma, o gerenciamento dos 4P's atualmente é um conceito altamente difundido para o departamento de TI, uma vez que, monitora e controla a maneira como a operação e a manutenção tratam estes recursos, ou seja, como eles estão operando e executando sua manutenção (Esmeraldo, 2014).

Mas diferentemente do gerenciamento a gestão dos 4P's se preocupa em assegurar a geração de valor para o negócio da organização, ou seja, isso muda o enfoque na tomada da decisão em relação ao como operar e mantê-los, sendo necessário quantificar e analisar, concomitantemente, as oportunidades, o custo, o risco e o desempenho, em cada momento do ciclo de vida (Esmeraldo, 2014).

Para melhor compreensão desta prática de gestão os 4P's, tratados no livro Service Design da biblioteca ITIL, passam a ser considerados como "ativos" que se bem projetados e orquestrados de forma a se inter-relacionarem para gerar valor para a organização.

Segundo a Norma ISO/IEC 55000 - Visão geral, princípios e terminologia (ABNT ISO 55000, 2014) "ativo é um item, algo ou entidade que tem valor real ou potencial, para uma organização." Onde o seu valor irá variar entre diferentes organizações e suas partes interessadas, e pode ser tangível ou intangível, financeiro, ou não financeiro.

No entanto, para o departamento de Tecnologia da Informação, TI, a gestão dos seus ativos vai além do conjunto de Normas ISO/IEC 55000, pois elas tratam apenas da gestão de ativos físicos de TI, o ITAM (Information Technology Asset Management) merece maior cuidado, uma vez que a sua gestão necessita de definições específicas para os requisitos de controle, que são necessárias para a gestão dos seus ativos, em específico para os ativos de software (Software Asset Management - SAM).

Assim, para tratar destas peculiaridades foi desenvolvido um conjunto de Normas ISO/IEC que definem requisitos de gestão para os ativos de TI. Tais Normas intitulam- se como ISO /IEC 19770 Information technology - IT asset management. Que composta por 3 padrões internacionais, se identificam como:

- ISO /IEC 19770-1 Information technology - IT asset management - Part 1 Management system requirements (ISO/IEC 19770-1, 2017);

Esta Parte 1, da Norma, especifica requisitos para um sistema de gerenciamento de ativos de TI dentro do contexto da organização (ITAM), referido como um “sistema de gestão de ativos de TI” (ITAMS).

- ISO /IEC 19770-2 Information technology - Software asset management - Part 2: Software identification tag (ISO /IEC 19770-2, 2015);

A Parte 2 da Norma, estabelece especificações para *software* de etiquetagem para otimizar sua identificação e gerenciamento.

ISO /IEC 19770-5 Information technology - IT asset management - Part 5: Overview and vocabulary (ISO/IEC 19770-5, 2015);

E a Parte 5 da Norma, fornece uma visão geral da família de normas ISO/IEC 19770, uma introdução ao gerenciamento de ativos de TI (ITAM) e gerenciamento de ativos de software (SAM), uma breve descrição dos princípios e abordagens da fundação nos quais o SAM é baseado, e por fim os termos e definições consistentes para uso em toda a família de normas ISO/IEC 19770.

Definido na Norma ISO/IEC 19770-5 (ISO/IEC 19770-5, 2015), o SAM é como uma atividade de controle e proteção de software e seus ativos relacionados dentro de uma organização; de controle e proteção de informações dos ativos que os mantêm, e se fazem necessários, para controlar e proteger estes ativos de software.

Assim, existem várias características dos ativos de TI que criam esses recursos adicionais e mais detalhados.

- Natureza do *software*: O *software* é um dos ativos mais importantes à ser gerenciado pelo ITAM, possuindo diversas características que criam requisitos de controle específicos:
- Facilidade na modificação, duplicação e distribuição de *software*: Isto porque o *software* é eletrônico ao invés de físico, podendo ele ser prontamente modificado, duplicado e distribuído criando grandes exposições e modificações não autorizadas (sendo elas maliciosa ou não maliciosa).

Em muitos aspectos, os ativos de *software* apresentam maior complexidade tecnológica do que os ativos físicos tais como:

- Flexibilidade de localização: o *software* pode ser armazenado ou instalado em um local, mas acessados ou utilizados a partir de instâncias ou locais adicionais.
- Número e complexidade dos componentes: há muito mais componentes para *software* do que para ativos físicos, existindo centenas de milhares de arquivos em um computador pessoal.

- Taxa de mudança: há uma alta taxa de mudança de *software*, sendo ela muito mais rápida do que a taxa de mudança de ativos físicos.
- Versão de componentes: existe um forte requisito para versionamento de *software*. Tais componentes precisam ser controlados por diversos propósitos, incluindo a segurança e compatibilidade com o ambiente corporativo.
- Medição de uso: muitas vezes, é desafiador medir o uso de *software*, que pode ser necessário para propósitos gerais de gerenciamento, bem como para conformidade contratual. A medição do uso de *software* pode, além disso, depender de hardware e outras medições.
- Licenciamento: o *software* geralmente está sujeito a termos e condições de licenciamento complexos. Embora muitos ativos físicos também possam estar sujeitos a termos e condições de licenciamento.
- entre outros.

Independente de tais peculiaridades listadas acima, tal gestão definida pelo conjunto de Normas ISO/IEC 19770 consiste em estabelecer o valor máximo para o uso dos ativos inventariados e definir qual o tamanho adequado para o inventário de TI, de forma a permitir a otimização de decisões e estratégias quanto a aquisição e o inventário destes ativos. Tal prática de gestão permite à organização obter uma visão holística do parque tecnológico de TI ajudando a organização a obter uma compreensão profunda de:

- Quais sistemas e equipamentos existem;
- Onde os componentes residem;
- Como eles são usados;
- Quanto eles custam;
- Quando eles foram adicionados ao inventário;
- Como eles estão dentro do ciclo de vida (prazo de validade);
- Como eles afetam os serviços de TI nos negócios.

Definir corretamente o nível de detalhamento no inventário de TI permite que a organização melhore a eficiência e o desempenho da infraestrutura de TI de forma a minimizar as despesas gerais relacionadas a manutenção destes ativos a longo prazo. Manutenção de ativos de TI se refere a manter a eficiência operacional através de configurações inteligentes que impossibilitem o mau uso dos ativos de TI por funcionários,

colaboradores e partes externas a organização. A implantação dos controles da ISO/IEC 27001 (ABNT ISO/IEC 27001, 2013) fecham estas lacunas uma vez que toda a infraestrutura já está sendo gerenciada e gerida através de melhores práticas e padrões Internacionais como os conjuntos de Normas ISO/IEC 55000 e ISO/IEC 19770.

O ITAM fornece uma base substancial para a implantação da segurança da informação. Um conjunto de requisitos de controle presentes na ISO/IEC 27001 está relacionado à segurança de equipamentos; três dos cinco principais controles críticos de segurança nomeados pelo *SANS Institute* envolve a criação de inventários de *hardware* de TI e *software*, a proteção de suas configurações e a avaliação e configuração contínua das vulnerabilidades existentes ao ambiente organizacional.

Porém, a velocidade da inovação tecnológica também leva à mudanças contínuas nos ativos de TI inseridos no ambiente organizacional, não deixando de fora os termos sob os quais eles são referenciados.

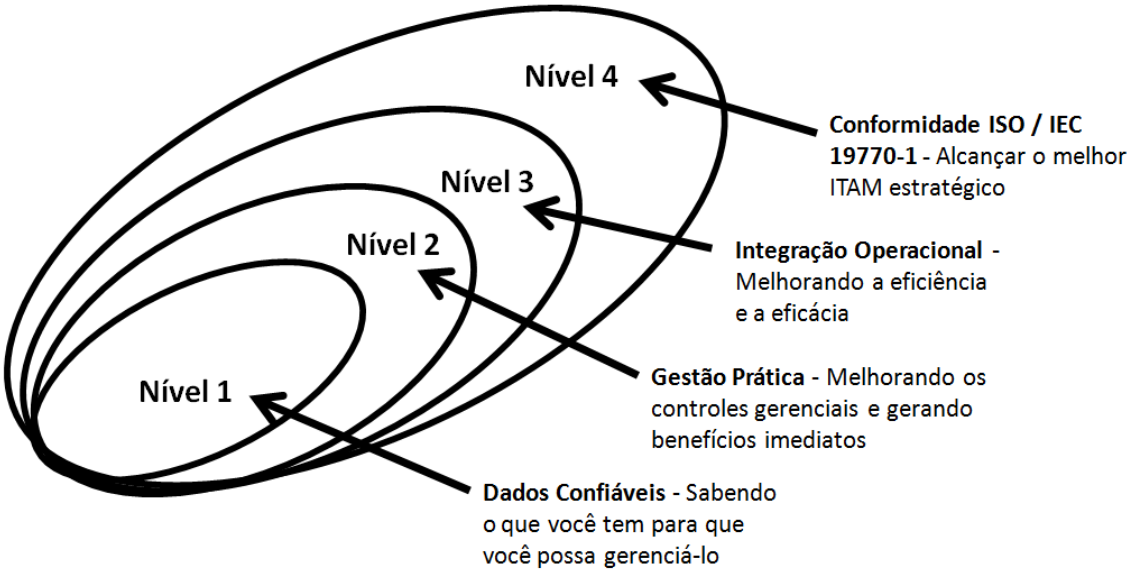
Os atuais mercados de ITAM *e* SAM são dominados por uma série de abordagens específicas de fornecedores para licenciamento, gerenciamento de licenças e otimização de ativos. Cada abordagem é única e emprega sua própria terminologia.

Embora essa abordagem possa estimular a inovação, também resulta em um consumidor de *software* sendo obrigado a lidar com cada um desses fornecedores em uma base de dados separada, o que leva à ineficiências significativas e evita comparações fáceis.

O ITAM e SAM são frequentemente executados por uma mistura de meios automatizados e manuais, mesmo em organizações de grande porte.

Para atingir os níveis de excelência do ITAM o anexo B da Norma ISO/IEC 19770-1 estabelece um controle de nível de maturidade para o processo de implementação, conforme Figura 2, que segue:

Figura 2 - controle por nível para uso com esta parte da ISO / IEC 19770.



Fonte: 1 ISO / IEC 19770

Onde:

- Nível 1: dados confiáveis. Alcançar esse nível significa saber o que você tem para poder gerenciá-lo.
- Nível 2: Gestão Prática. Alcançar esse nível significa melhorar os controles gerenciais e gerar benefícios imediatos.
- Nível 3: Integração operacional. Atingir este nível significa melhorar a eficiência e a eficácia.
- Nível 4: Conformidade total com ISO / IEC 19770-1. Alcançar esse nível significa atingir o melhor ITAM estratégico da categoria.

1.1. GESTÃO DE ATIVOS

Com a demanda das indústrias para adotar um padrão de gestão de ativos e definição de estratégias para a gestão que englobassem desde o ciclo de vida até a manutenção diária (custo /risco /desempenho) em 2004 foi publicada pela British Standars Instituition (BSI) o PAS 55 (Publicly Available Specification) (BSI PAS 55-2, 2008). Porém não obstante da sua publicação, em 2008, a PAS 55 sofre revisão. Liderada pelo Institute of Asset Management participaram desta revisão 50 organizações de 15 setores da indústria sediados em 10 países; mesmo tendo 28 requisitos e definições bem

claras, o PAS 55 não é uma Norma com força de ser auditada por organismo externo "certificador" que validaria a conformidade com requisitos para emitir o selo de certificação.

A fim de se tornar uma Norma de uso Internacional para atendimento, não somente aos serviços públicos de gás, eletricidade e água, sistemas de transporte rodoviário, aéreo e ferroviário, instalações públicas, processos, manufatura e indústrias de recursos naturais, em 2010 foi fundado o comitê de Projeto ISO251 com sua primeira reunião em Melbourne.

Em 5 de fevereiro de 2014 em Londres foram lançados os três padrões internacionais que permearam a gestão de ativos que a PAS 55 defendia nos seus requisitos de manutenção: a ISO/IEC 55000, ISO/IEC 55001, e ISO/IEC 55002 (ABNT ISO 55000, 2014); definiremos que a "Norma ISO/IEC 55000" se refere ao conjunto de Normas anteriormente citados.

Com o objetivo de ser um conjunto de Normas que fornece diretrizes para a aplicação de um sistema de gestão para gestão de ativos, a Norma ISO/IEC 55000 permite que uma organização alcance:

- um melhor o gerenciamento de risco;
- registros que permitam definir a rastreabilidade dos ativos;
- o valor do ativo através do seu uso ótimo em todo seu ciclo de vida;
- o aumento da disponibilidade dos ativos;
- a redução dos custos em reparos e aumento de produtividade;
- a melhoria do planejamento das ações sob os ativos;
- a qualidade dos serviços prestados aos clientes;
- a maximização dos resultados da empresa;
- a segurança e conformidade com as regulamentações;
- o cumprimento com a responsabilidade social e corporativa;

CONCLUSÃO

Organizações buscam novas tecnologias com o intuito de tornar os processos mais eficientes e eficazes, buscando ao máximo a redução de custos, tornando-se prioridade a otimização dos investimentos e a minimização dos riscos relacionados a TI.

Desta maneira a gestão de ativos aliada à gestão de riscos é fator preponderante para garantir bons resultados financeiros ou para avaliar o nível de exposição ao risco assumido pela empresa através da decisão de não investir ou renovar os ativos no momento necessário.

Com base neste cenário, este trabalho abordou de maneira abrangente as implicações legais que uma organização poderá estar vulnerável quando esta não fizer uma gestão eficaz e efetiva dos recursos de TI.

E assim, ao longo deste trabalho foi apresentado os benefícios alcançados pela aliança de implementação da ISO/IEC 55000 e ISO/IEC 19770 resultando um alcance completo de todos os ativos de TI.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 55000:2014 Gestão de ativos - Sistemas de gestão - Diretrizes para a aplicação da ABNT NBR/ISO 55001**, 2014

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO 55001 - Gestão de ativos — Sistemas de gestão — Requisitos, 2014

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO 55000 - Gestão de ativos — Visão geral, princípios e terminologia, 2014

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001 - Sistemas de gestão de segurança da Informação- Requisitos. 2013

BSI PAS 55-2 2008 Asset Management

ESMERALDO, João; KARDEC, Alan; LAFRAIA, João R.; NASCIF, Julio. Gestão de Ativos. 1a. ed. - Rio de Janeiro: Qualitymark Editora, 2014.

HIGOR. J. et.al. Segurança Corporativa: guia de referência. São Paulo: OAB-SP. 2015.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. Código das melhores práticas de governança corporativa. 5ª. ed. Disponível em: http://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=21138. Acesso em: Dezembro. 2018.

ISO /IEC 19770-2:2015 Information technology - Software asset management - Part 2: Software identification tag

ISO/IEC 19770-1:2017 Information technology - Software asset management - Part 2: Software identification tag

ISO/IEC 19770-5:2015 - Information technology - Software asset management - Part 5 Overview and vocabulary

KPMG. MAPA DAS FRAUDES. Disponível em: <https://assets.kpmg.com/content/dam/kpmg/br/pdf/2016/12/br-kpmg-business-magazine-39-fraude.pdf>. Acesso em: Novembro 2018.

TAYLOR, Sharon; LLOYD, Vernon; RUDD, Colin. ITIL Service Design. APMG, 2011.