risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 14/01/2022
Aceitação/Acceptance: 20/05/2022

Impacto de processos tecnológicos na segurança de sistemas: enfoque em micro, pequenas e médias empresas

Adolfo Alberto Vanti[1], Pedro Solana-González[2], Sidia Maria Callegari-Jacques[3]

avanti@pq.cnpq.br; pedro.solana@unican.es; sidia.jacques@ufrgs.br

[1] Pesquisador CNPq / Proj. Universal, Brasil

[2] Universidad de Cantabria, Av. de los Castros, s/n, Santander 39005, Cantabria, España

[3] Universidade Federal do Rio Grande do Sul, Av. Paulo Gama, 110, Bairro Farroupilha, Porto Alegre, Rio Grande do Sul, 90040-060, Brasil

Pages: 1-20

Resumo: Este trabalho analisou o impacto de processos tecnológicos para o aumento das garantias de segurança de sistemas junto à 180 micro, pequenas e medias empresas situadas no sul do Brasil. Para tal se utilizou de análise quantitativa de níveis de maturidade de processos do modelo COBIT. Se revisou teoricamente as principais versões do COBIT e segurança de sistemas e metodologicamente foram usadas técnicas estatísticas de correlação linear simples de Pearson, correlação não paramétrica de Spearman e regressão linear simples e múltipla. Os achados em gestão estão relacionados com o processo tecnológico de conformidade dos requisitos externos para gerar aumento das garantias de sistemas, entre outros processos que relacionados trouxeram importância secundária ao processo decisório.

Palavras-chave: Segurança dos sistemas; Processos tecnológicos; COBIT; PME.

Impact of technological processes on system security: focus on micro, small and medium-sized enterprises

Abstract: This work analysed the impact of technological processes to increase system security guarantees for 180 micro, small and medium-sized companies located in southern Brazil. To this end, a quantitative analysis of the process maturity levels of the COBIT model was used. The main versions of COBIT and system security were theoretically reviewed and statistical techniques of simple linear correlation of Pearson, non-parametric correlation of Spearman and simple and multiple linear regression were used methodologically. The findings in management are related to the technological process of compliance of external requirements to generate an increase in system guarantees, among other related processes that brought secondary importance to the decision-making process.

Keywords: Systems security; Technological processes; COBIT; SME.

1. Introdução

A relação de processos tecnológicos com a segurança de sistemas impacta de maneira diferenciada para empresas variando o porte, o setor empresarial, a norma estudada, o framework e estratégia empresarial. O setor financeiro trata a informação de maneira muito estratégica, as empresas exponenciais da mesma maneira pois esse ativo vende mais, vende melhor e muitas vezes automaticamente. Normas ISO de segurança da informação ou instrumentos como o COBIT, aqui estudado como mesmo na sua versão mais recente, a versão 2019 (ISACA, 2021), procuram integrar de maneira operacional ao estratégico a importância devida da informação bem como sua proteção.

Assim, o enfoque na segurança dos sistemas é uma abordagem com impacto estratégico na qual as instituições convertem dados operacionais em ativos extremamente valiosos. Neste trabalho se analisam com ferramentas estatísticas os dados de maturidade em processos tecnológicos de 180 micro, pequenas e médias empresas para compreender melhor esse diálogo entre processos de TI e segurança, de maneira mais macro que extrapola as próprias fronteiras de estudos organizacionais por ser uma análise mais setorial.

O conjunto de normas internacionais ISO 27000 sobre segurança da informação e COBIT (principalmente as versões 4.1, 5 e 2019) geram controles em sistemas e processos operacionais tecnológicos que buscam aumentar as garantias de Governança de Tecnologia da Informação (GTI) e de Governança Corporativa (GC) (OECD, 2018) através de adequada maturidade em processos tecnológicos (Debreceny & Gray, 2013) e da difícil governança da própria segurança da informação (Slayton, 2021) mas que trate de sua incerteza de seu gerenciamento através de análise de riscos.

Um dos aspectos importantes no controle e gerenciamento de dados refere-se à aplicação de técnica quantitativa estatística com o uso do SPSS que nesse trabalho foi realizado junto ao processo DS5 (Garantir Segurança dos Sistemas), analisado neste estudo. O COBIT é um modelo de avaliação de processos tecnológicos para fins de controle, amplamente utilizado que e em sua versão 4.1 apresenta seus 4 domínios consideram Planejamento e Organização (PO), Aquisição e Implementação (AI), Entrega e Suporte (DS) e Monitoramento (MO). Referido framework possui etapas de evolução, porém a base de dados analisada está relacionada com esta versão.

Se apresenta com versões diferentes como a versão 5 cascateando muito bem os objetivos corporativos aos tecnológicos de maneira integrada e agregando valor em benefícios, custos/riscos e recursos, mas com limitações na operacionalidade dos habilitadores. A Tabela 1 da continuação apresenta os objetivos de TI relacionados com as dimensões ou perspectivas do *Balanced Scorecard* (BSC) (Kaplan & Norton, 2004).

A versão mais recente do COBIT nos traz um diálogo melhor com a terminologia de estratégia, da visão do gestor com maior protagonismo frente aos processos tecnológicos e assim o próprio framework vai se transformando mais em objetivos do que processos porque há maior consciência que a empresa não pode ser encarada somente com a visão de processos, mas que se necessita permanentemente melhorar o processo decisório (Simon, 1961).

Dimensão BSC de TI	Objetivo da Informação e Tecnologia Relacionada	
Financeira	01	Alinhamento da estratégia de negócios e de TI
	02	Conformidade de TI e suporte para conformidade do negócio com as leis e regulamentos externos
	03	Compromisso da gerência executiva com a tomada de decisões de TI
	04	Gestão de risco organizacional de TI
	05	Benefícios obtidos pelo investimento de TI e portfólio de serviços
	06	Transparência dos custos, benefícios e riscos de TI
Cliente	07	Prestação de serviços de TI em consonância com os requisitos de negócio
	08	Uso adequado de aplicativos, informações e soluções tecnológicas
Interna	09	Agilidade de TI
	10	Segurança da informação, infraestrutura de processamento e aplicativos
	11	Otimização de ativos, recursos e capacidades de TI
	12	Capacitação e apoio aos processos de negócios através da integração de aplicativos e tecnologia
	13	Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos
	14	Disponibilidade de informações úteis e confiáveis para a tomada de decisão
	15	Conformidade de TI com as políticas internas
Treinamento e Crescimento	16	Equipes de TI e de negócios motivadas e qualificadas
	17	Conhecimento, expertise e iniciativas para inovação dos negócios

Tabela 1 – Objetivos da informação e tecnologia nas dimensões do BSC.
Fonte: Elaboração própria, com base em Bernard (2012)

Estes autores defendem isso há muitos anos frente a algumas visões limitadas, visões mais técnicas que muitas vezes não conseguem gerenciar as atividades de maneira complexa e holística e que não percebem fenômenos emergentes estratégicos (Mintzberg, 1994), criativos e inovadores do conhecimento empresarial (Davenport & Prusak, 1998) e da geração de resultados complexos (Bonabeau, 2002). Estes fenômenos são os relacionados na empresa ao alinhamento estratégico em que são significativos (Morin, 2003) em pequenas variações, mas geram grandes impactos na vantagem competitiva (Argyris, 1996; Porter, 1990) e na segurança de sistemas pois com a pandemia Covid-19 cresceram muito as fraudes virtuais.

Isso também se reflete nas garantias de práticas de adequada governança corporativa, esta considerada como um significativo sistema que dirige e monitora processos organizacionais envolvendo principalmente os relacionamentos entre sócios, conselho, diretoria, órgãos de fiscalização e controle junto a stakeholders (IBGC, 2020). E se amplia também necessariamente quando se considera a cultura organizacional e a organização como um ser vivo (Morgan, 1986), com fatores homogêneos e heterogêneos (Schein, 1992), com comportamentos até antropológicos, ideológicos e sociológicos de

história, mito e lenda (Peters & Waterman, 1982). Assim sociedades mais individualistas ou de grupo como as diferentes culturas nacionais que impactam nas organizações se apresentam, desde a individualista norte americana até a grupal cultura japonesa ou mesmo passando pelas culturas de sociedades latinas da busca prioritária por emprego estável (Hofstede, 1984).

Assim, esse alinhamento estratégico que é recuperado na versão do COBIT 2019 se estabelece frente à cultura forte ou fraca do trabalho com seus comportamentos de liderança, valores, crenças, linguagens, ritos, símbolos, regras sociais entre outros aspectos (Peters & Waterman, 1982), (Morgan, 1986; Schein, 1992).

Sendo assim a segurança acaba sendo tratada de maneira secundaria mas que vem se invertendo muito na última década com a participação dos próprios usuários (Bulgurcu, Cavusoglu, & Benbasat, 2010; Spears & Barki, 2010) que são tratados como os recursos mais valiosos na gestão de risco da segurança de informações mas que falham muito nos capítulos dessas normas quando se referem a Recursos Humanos pois possuem um enfoque muito técnico e limitado que se caracteriza em um ciclo entrópico com pouca visão estratégica e aos objetivos corporativos. Esta visão, porém, também pode ser analisada de diferente maneira pois os funcionários principalmente com a pandemia sanitária apresentam comportamentos de desengajamento e comportamentos contraproducentes em suas responsabilidades com a informação (Hadlington, Binder, & Stanulewicz, 2021).

O problema de pesquisa formulado neste trabalho é: quais processos tecnológicos mais impactam na Segurança de Sistemas considerando uma análise junto a micro, pequenas e médias empresas? Este problema é respondido nesse estudo considerando de maneira operacional, mas atendendo à consciência estratégica cultural das organizações. Para tal, de maneira prática, foram examinados esses processos em uma extração de 180 empresas do setor industrial localizadas principalmente no sul do Brasil, nas quais as relações entre os processos tecnológicos foram analisadas com o uso de técnicas estatísticas de correlação linear simples de Pearson, correlação não paramétrica de Spearman e regressão linear simples e múltipla.

Por fim, o trabalho está estruturado e uma revisão da literatura com segurança de sistemas e processos tecnológicos para logo alcançar a metodologia e o posicionamento de análises via correções e regressões com o uso intensivo de SPSS para finalmente apresentar os resultados da pesquisa, conclusões e referências bibliográficas.

2. Revisão da literatura

Nesta revisão foram contemplados temas relacionados à segurança de sistemas e processos tecnológicos considerando análise do COBIT.

2.1. Segurança de sistemas

Segurança de sistemas está completamente integrada com segurança da informação praticamente como sinônimos pois segurança de sistemas atua na segurança da mesma, dos ativos da informação que tanto as empresas preservam atualmente. A segurança de sistemas é estratégica porque se falha o sistema, falha a estratégia, falha a empresa

e muito em sua integridade da informação na confidencialidade (Dhillon & Backhouse, 2000) e disponibilidade. Pontos-chave são importantes para minimizar problemas de cibersegurança como os analisados em relatórios Europol (2020) (Internet Organized Crime Threat Assesment) de *ransomware*, *malware*, CaaS, engenharia social que tenta manipular funcionários para colocar em risco a segurança de sistemas (Grassegger & Nedbal, 2021), *phishing* e BEC.

Estas falhas, que podem variar muito, são avaliadas de maneira organizacional com estudos de caso em diferentes empresas ou de maneira externa em comparativos entre empresas, como analisado neste trabalho. A forma aqui que se avaliou o nível de impacto de processos tecnológicos em segurança de sistemas se dá através de níveis de maturidade com base no modelo COBIT (Young & Windsor, 2010). Então, a segurança de sistemas está ligada as normas ISO/IEC 27002: 2007 e ISO/IEC 27032: 2012 que objetivam eliminar os riscos de falta de segurança da informação (Shamala, Ahmad, Zolait, & bin Sahib, 2015), controles de seguridade (Rohn, Sabari, & Leshem, G., 2016), diretrizes para a segurança em internet e cibersegurança (Malatji, Marnewick, & Von Solms, 2021) e melhoria da conformidade das informações (Buccafurri et al., 2015; Safa, Von Solms & Furnell, 2016), porque os sistemas muitas vezes não são projetados prioritariamente para serem seguros mas para resolverem problemas organizacionais.

Com isso é realizada a conexão entre TI e estratégica em forma de cascata como defendido em COBIT cujos objetivos de TI se relacionam aos objetivos corporativos do BSC (Kaplan & Norton, 2004), proporcionando maior conformidade, transparência, prestação de contas e redução de risco (IBGC, 2015; ISACA, 2018; OECD, 2018) à empresa.

Assim que bancos e financeiras possuem alto nível de maturidade de seus processos tecnológicos pois dessa forma garantem segurança de sistemas e boas práticas de governança corporativa de tecnologia da informação, podendo realizar alinhamento estratégico de maneira mais eficaz sem perder robustez de sua origem conceitual na governança de TI que são os direitos de decisão e de matriz de responsabilidades para motivar comportamentos desejáveis no uso da TI de uma empresa (Weill & Ross, 2005; ITGI, 2003). Este enfoque é multidisciplinar na empresa se integrando com outros processos como a *accouting information systems* (Wilkin & Chenhall, 2010) que gerencia a previsão de investimentos em estruturas, pessoas e mecanismos relacionados, reduzindo-se retrabalhos e decisões equivocadas e pouco tempestivas que conduzem a riscos financeiros, operacionais, tecnológicos entre outros que afetem diretamente seus ativos.

Nesse trabalho, esses níveis de maturidade foram caracterizados pelas análises COBIT (ISACA, 2018) e, mais especificamente ao processo tecnológico DS5 - Segurança de Sistemas -, em aplicações sobre 180 empresas brasileiras de diferentes setores. Com essas análises pode-se também "girar" diversas análises como verificar o impacto de processos envolvendo RH na segurança de sistemas. Salienta-se isso porque muitas vezes tecnicamente esse enfoque é muito limitado pois alcançar uma conformidade corporativa também depende de uma sustentação na gestão da cultura organizacional (Morgan, 1986) e de proteção de dados pois os funcionários podem desenvolver aplicações de TI que vão além daquelas somente relacionadas com indicadores de desempenho.

O profissional de gestão, assim, avança rapidamente alinhando atividades variadas de boas práticas de TI, governança e estratégia com conceitos tecnológicos robustos de segurança de sistemas, redefinindo sua própria formação e atuação em mercado tão competitivo e que deve prestar contas a diversos órgãos regulatórios como o atual.

2.2. Processos tecnológicos

Os processos operacionais são gerenciados e monitorados para que estejam bem dimensionados, bem estruturados e com isso se possa desenvolver aplicações de sistemas mais robustas (Alkhaldi, Hammami, & Uddin, 2017) e mais adequadas à governança corporativa. Isso se dá com o atendimento de requisitos e aumento de segurança de sistemas através da governança tecnológica (ISACA, 2012) onde se posiciona e atua o modelo COBIT (ISACA, 2018).

O COBIT 2019 nos amplia o enfoque de requisitos da informação que regulam a segurança dos sistemas e os processos tecnológicos numa agregação de valor alcançando os requisitos de precisão, objetividade, credibilidade, reputação, relevância, amplitude, atualização, adequação, concisa, consistente, interpretável, compreensível, manuseável e informação restringível quando necessária (ISACA, 2021). Estes requisitos atendem a uma GTI (Weill & Ross, 2005, pp. 2-11; ITGI, 2003) e uma GC que é tão necessária desde alguns anos atrás devido principalmente às crises financeiras e escândalos econômicos já tão difundidos na literatura mas que dá continuidade em uma integridade de processos respeitando a governança local em diferentes aplicações como no ensino superior (Gerl, von der Heyde, Groß, Seck, & Watkowski, 2021) e na qualidade de serviço nesse mesmo tipo de instituição (Justitiaa, Zaman, & Putra, 2021).

Dessa forma foi possível realizar um diagnóstico dos domínios e respectivos processos, que neste estudo focou no DS5 - Garantir Segurança dos Sistemas - (Aguiar, Pereira, Vasconcelos & Bianchi, 2018), e foi obtida pela aplicação de *framework* do COBIT (ITGI, 2007) em 180 empresas que operam em diferentes setores de produção (maior parte em indústrias metal-mecânica, química e calçadista), situadas principalmente na região sul do Brasil. Logo foi realizado um recorte final para a análise estatística de micro, pequenas e médias empresas, excluindo-se as grandes empresas.

Assim, a garantia de sistemas DS5 está classificada no domínio Entrega e Suporte (DS), o qual se refere à entrega dos serviços solicitados, incluindo entrega de serviço, gerenciamento da segurança e continuidade, serviços de suporte para os usuários e o gerenciamento de dados e recursos operacionais. Esta estrutura de gestão da informação e da governança tecnológica do COBIT não pode ser tratada de maneira simplista, o que nos levou a usar técnicas estatísticas de correlação e regressão linear múltipla, que geraram resultados estatisticamente significativos e com aplicação prática potencial interessante.

COBIT 2019 é mantido pela *Information Systems Audit and Control Foundation* (ISACA), instituição sem fins lucrativos que possui participantes em torno de 140 mil profissionais distribuídos em 188 países. Esse framework possui a sua versão mais recente a do ano de 2019 (ISACA, 2021) e com ela se adapta ainda melhor à visão de negócios (mais informação que tecnologia), às pequenas e médias empresas, às novas

demandas do mercado e tecnológicas sem perder robustez de sua estruturação de avaliação de processos de TI que já vinha evoluindo em versões anteriores. Também considerou instrumentos de aplicação como a matriz de responsabilidades RACI – *Responsible*, *Accountable*, *Consulted*, *Informed* – no mapeamento de processos na versão anterior (a versão 5), bem como o mapeamento dos objetivos corporativos com o de TI conforme a Figura 1 da continuação.

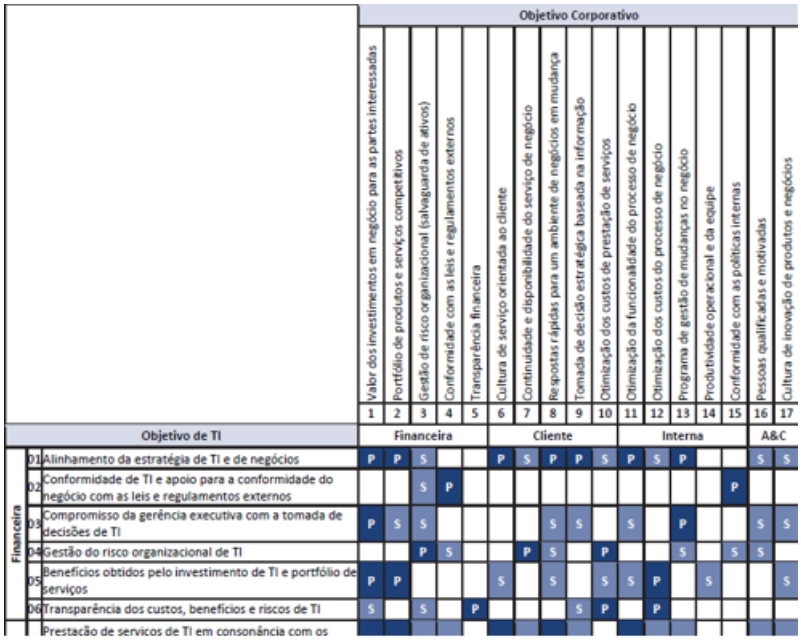

Figura 1 – Mapeamento dos objetivos corporativos com os de TI.
Fonte: ISACA (2012)

Para ISACA, COBIT é um modelo para a governança e gestão de tecnologia da informação empresarial para alcançar suas estratégias, objetivos e metas corporativas de TI em uma organização, sendo também considerado um modelo de boas práticas.

Conforme ISACA o COBIT 2019 em relação às outras versões mantém conceitos chave e recupera o conceito de alinhamento, avalia a capacidade do processo também recuperando o CMMI – *Capability Maturity Model Integration* –, conduz ao código aberto, direciona o fator de Design, define áreas de foco como PMEs e transformação digital com código aberto e colaborativo. Assim, os objetivos de governança e gestão estão alinhados aos objetivos da empresa e estes estão relacionados a um processo e a um conjunto de Componentes. São 40 objetivos nos quais 5 são de governo/governança e 35 são de gestão, distribuídos agora nos domínios de acordo com a EDM – *Evaluate*, *Direct*, *Monitoring* – agrupando os Objetivos de Governo e os Objetivos de Gestão nos domínios chamados APO, BAI, DSS e MEA.

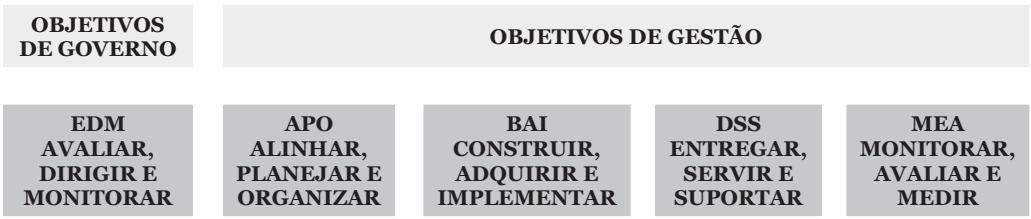

Figura 2 – Objetivos de governança e gestão do COBIT 2019.
Fonte: (ISACA, 2021)

Assim, com um maior enfoque de alinhamento estratégico do COBIT 2019 para o posicionamento Porteriano de diferenciação é que situa a empresa no mercado perante as incertezas de riscos (ISACA, 2021). Porém isso não garante que a mesmo alcance e mantenha esse posicionamento porque além das forças que influenciam toda uma cadeia e rede de valores, também a empresa depende de um mergulho organizacional em sua cultura, seus comportamentos e nas relações com as forças estratégicas (Morgan, 1986; Schein, 1992).

Esse posicionamento interno pode ser inserida em sistemas através do desenvolvimento de uma cultura mais densa em seus funcionários desde que a mesma seja trabalhada de maneira consciente, envolvendo inclusive diferentes tipos de ritos como de passagem, de degradação, de confirmação, de reprodução, de redução de conflito e de integração (Beyer & Trice, 1987) e caracterizando uma cultura organizacional com seus diferentes níveis como o de artefatos visíveis, dos valores que governam os comportamentos das pessoas e do nível de pressupostos inconscientes (Trice & Beyer, 1984).

Empresas procuram melhorar continuamente suas forças e fraquezas, procuram entender melhor as oportunidades e ameaças, mas conectam insistentemente a SWOT – *Strength, Weakness, Opportunities and Threats* – nela mesma sem conectar-se com objetivos e ações da empresa. Desta forma desconsideram ou consideram de maneira limitada as relações de incidência e de pertinência difusas e assim operam de maneira muitas vezes descoladas com a realidade de mercado. Já o alinhamento via BSC liderado por Kaplan e Norton (2004) atende bem a cascada de objetivos corporativos de maneira linear, mas não alcança bem a SWOT nas suas interligações. Então, há a preocupação que se continue alinhando a área operacional com a estratégica e com a governança de maneira mais coerente com as complexidades que o mercado impõe.

O que se conhece muito e de maneira também prática é desenvolver cálculos de médias aritméticas que não representam bem a complexidade organizacional por não perceberam o efeito de complexidade como o efeito "borboleta" em que pequenas diferenças nas condições iniciais de um sistema dinâmico podem ter um efeito enorme no resultado deste mesmo sistema (Gleiser, 2002). Por isso, é necessário ampliar para cálculos diferenciados passando por médias geométricas e/ou envolver técnicas como a lógica difusa (Klir, Clair, & Yuan, 1997; Zadeh, 1965) sustentada pela teoria dos conjuntos que possibilitam desenvolver o trato de dados e informações como um processo colaborativo

externo de incidência e que permitem a um entendimento da aprendizagem contínua (Argyris, 1996) que inove com novos produtos junto ao mercado.

Assim, uma estratégia pretendida sofrerá menos influências de incertezas que as convertem em estratégia realizada, principalmente devido a eventos ambientais, mas também aos eventos organizacionais de investimentos como em pessoal que provocam as mudanças (Mintzberg, Ahlstrand, & Lampel, 1998; Prahalad & Hamel, 1990) significativas que a empresa necessita.

Para desenvolver esse aculturamento e consciência do trato da segurança de sistemas junto aos processos tecnológicos é que esse trabalho atua, com técnica estatística para reduzir as instabilidades ocasionadas nos sistemas de informações, mas também além disso, desenvolver enfoques em que se aumente as garantias de segurança de sistemas que fazem parte de uma governança corporativa e de TI e consequentemente da estratégia da empresa.

Conforme Wright, Kroll e Parnell (1998, p. 24), estratégia refere-se aos planos da alta administração para alcançar resultados consistentes com a missão e os objetivos gerais da organização, podendo-se encarar a estratégia de três pontos de vantagem: a formulação da estratégia, a sua implementação e o controle estratégico.

Neste trabalho foram realizadas análises em base de dados com técnica estatística de correlação e regressão. Resultados consistentes foram encontrados que impactam estrategicamente as instituições avaliadas sob esse enfoque e sob diversas perspectivas tanto técnicas, quando de entrega de serviços, de planejamento e organização e mesmo comportamental. Dessa forma, a transformação de todo o conhecimento da empresa em valor para ela exige um ambiente transparente e seguro em que a alta maturidade no desenvolvimento de processos de negócios e os tecnológicos manterá a empresa competitiva (Raisinghani, 2000). Estas estão explicadas na metodologia e aplicadas na sua sequência.

3. Metodologia

A metodologia utilizada no modelo computacional que avaliou a segurança de sistemas através do processo DS5 em processos tecnológicos do *framework* internacional COBIT que alcança a GTI e que atende à estratégia organizacional foi quantitativa, com técnicas estatísticas de correlação e regressão linear múltipla. Assim se objetivou analisar o impacto dos processos tecnológicos com as garantias de segurança da informação através de níveis de maturidade (0 a 5) e assim integrar aspectos operacionais de sistemas com a estratégia empresarial.

A aplicação estatística realizada também foi convergente com um processamento de mineração de dados que possibilita o aprendizado de máquina (Farazzmanesh & Hosseini, 2017). Assim, a coleta de dados realizada gerou uma base que vem sendo alimentada desde 2012 com empresas, as quais participam/colaboram em atividades e projetos de várias universidades, sendo que destas vem evoluindo nos melhores frameworks de governança de TI ou corporativa de TI como é o COBIT. Os níveis de maturidade da empresa são assim distribuídos:

0. – *Inexistente*: Neste nível há uma absoluta falta do processo. A organização não tem conhecimento sobre as implicações que a falta do processo pode gerar.
1. – *Inicial*: Neste nível os processos são esporádicos e desorganizados, não existe documentação e controle algum.
2. – *Repetitivo*, mas intuitivo: Neste nível os processos seguem um padrão de regularidade, com alta dependência do conhecimento dos indivíduos.
3. – *Definido*: Neste nível os procedimentos estão estabelecidos e são cumpridos. Inicia o uso de indicadores para controle.
4. – *Gerenciado*: Neste nível os processos estão integrados e alinhados. As metas e planos são baseados em dados e indicadores consistentes.
5. – *Otimizado*: Boas práticas são seguidas e automatizadas, com base em resultados de melhoria contínua.

As avaliações realizadas pelos respondentes se deram via escalas Likert em *survey* (com os escores variando entre 0 e 5) e alcançou a totalidade dos 34 processos de empresas diferentes. Para se avaliar o impacto de diversos processos tecnológicos sobre o processo específico que foi foco deste trabalho (DS5 – Garantir Segurança dos Sistemas), foram consideradas avaliações envolvendo 10 processos de Planejamento e Organização (PO), sete de Aquisição e Implementação (AI) e quatro de Monitoramento (MO), em um total de 21 processo.

O processo DS5 de garantia de segurança de sistemas estabelece uma relação de pertinência e de associação com os demais e estes com ele, gerando uma melhor GC e GTI e consolidando melhor a estratégia empresarial porque os objetivos de negócio estão ligados aos objetivos de TI. Dessa forma, os processos foram tratados com técnicas estatísticas que associaram as potencialidades entre eles e assim pode-se decidir sobre investimentos e prioridades para tratar as vulnerabilidades de processos tecnológicos.

Complementarmente, a análise quantitativa permite ao decisor compreender também a hierarquização e as conexões entre os diferentes processos tecnológicos e essas relações para a melhoria do processo decisório (Simon, 1996). Esse relacionamento também se dá entre os componentes do COBIT visando aos objetivos de negócios, que, em forma de cascata, descem para atividades-chave, formas de medição (onde está a maturidade), controle de resultado de testes e objetivos de controle.

Para responder à questão de quais processos tecnológicos mais impactam na segurança de sistemas e consequentemente na estratégia e governança, se utilizou uma análise quantitativa envolvendo o processo DS5 – Garantir Segurança dos Sistemas do COBIT. Assim, analisando os processos tecnológicos que têm maior repercussão na segurança de sistemas podemos aumentar a garantia deles, e como resultado garantir uma boa prática de governança de TI e consolidação da estratégia organizacional.

Para a análise quantitativa, foram usadas técnicas de correlação linear simples de Pearson, correlação não paramétrica de Spearman e regressão linear simples e múltipla através do software SPSS v.18.

3.1. Técnicas de correlação e regressão

A análise da relação entre variáveis depende do tipo de variável utilizada. Entre variáveis quantitativas, usam-se técnicas de correlação e/ou regressão. Com o coeficiente de

correlação de Pearson se avalia o quanto as alterações em uma variável estão associadas a mudanças em outra. Correlação não implica em causalidade, que envolve aspectos filosóficos e metodológicos mais elaborados. Mas a presença de correlação estatística entre duas variáveis mostra indícios de uma relação entre elas que possa ter interesse prático.

A análise inicia com a elaboração de um diagrama de dispersão de pontos, seguido do cálculo do coeficiente de correlação e finalmente o teste de sua significância estatística. O coeficiente de correlação produto-momento de Pearson "r" e deste ponto em diante simplesmente "coeficiente de correlação" que mede o grau de associação entre as duas variáveis quantitativas.

O teste estatístico do coeficiente de correlação permite calcular a probabilidade de que um valor igual ou maior do que o obtido seja observado caso não exista correlação ente as variáveis. Esta probabilidade é geralmente denominada valor-P, ou simplesmente P e ela é calculada supondo que não existe correlação entre X e Y. Se o valor-P for baixo, digamos 0,05, indica que se na verdade não houver correlação, a probabilidade de ocorrer, em uma amostra aleatória, um valor tão ou mais alto que o obtido é no máximo 0,05. O teste do coeficiente de correlação é um teste "t" de Student.

O coeficiente de Pearson é um teste paramétrico em que o pressuposto mais importante é o de que os dados das duas variáveis são provenientes de uma população onde a distribuição é bivariada Normal. No gráfico de pontos, esta distribuição aparece como uma nuvem elíptica. Se esse não for o caso, calcula-se e testa-se o coeficiente de correlação não paramétrico de Spearman (Dancey & Reidy, 2019). Este coeficiente mede a correlação entre os postos ou posições de cada valor da variável em relação aos demais valores da mesma. Para testar este coeficiente, as pressuposições são mais "frouxas" que as necessárias para testar o coeficiente de correlação de Pearson.

A análise de regressão amplia a análise de correlação e produz um coeficiente de regressão "b", que indica qual a aumento (ou decréscimo) esperado em Y para o aumento padrão de uma unidade na variável X. A regressão de Y sobre X é representada pela linha que passa à menor distância de todos os pontos. Assim como para o coeficiente de correlação, a conclusão sobre a dependência estatística de Y em relação a X está sujeita ao erro amostral. O teste de significância do coeficiente de regressão é um teste "t" de Student e o valor-P resultante mede a probabilidade de ocorrer o coeficiente de regressão observado (ou um ainda mais extremo) caso não haja dependência de Y em relação a X.

Em uma extensão desta análise, é possível avaliar o efeito de várias variáveis (designadas X1, X2, X3 etc.) sobre a variável dependente (Y). Na análise de regressão linear múltipla, os coeficientes de regressão são coeficientes Cada um indica o incremento esperado em Y para o aumento de uma unidade no preditor, levando em conta (ou ajustando pela) a presença das demais variáveis X no modelo de regressão múltipla.

A regressão múltipla é usada para se avaliar o efeito geral de um conjunto determinado de variáveis sobre Y ou para avaliar o efeito de uma variável X específica, controlando por outras que podem confundir o efeito do preditor. Nesta análise, o teste do efeito de cada variável é "t" de Student parcial e o resultado está sempre ajustado pela presença das demais variáveis X no modelo.

No presente estudo foram realizadas, inicialmente, análises de correlação entre a variável de interesse DS5 e cada um dos processos dos domínios PO (10 processos), AI (7) e MO (4), totalizando 21 processos. A seguir, foram efetuadas três análises de regressão múltipla, uma para cada domínio, em que Y foi DS5 e X foram todos os processos do domínio em análise. Finalmente, o processo mais relevante de cada um dos três domínios foi selecionado e as três foram analisadas conjuntamente em uma análise de regressão múltipla. Em todas as análises, o nível de significância escolhido foi 0,05.

4. Resultados

O problema de pesquisa se referia a: quais processos tecnológicos mais impactam na segurança de sistemas? Este foi o problema definido de pesquisa e para respondê-lo se utilizou uma análise quantitativa envolvendo o processo DS5 de segurança de sistemas do COBIT. Assim, objetivando analisar processos tecnológicos que mais impactam na segurança de sistemas podemos aumentar a garantia deles, e consequentemente garantir uma boa governança de TI e alcançar a estratégia organizacional.

Os coeficientes de correlação de Pearson (r) e não paramétrico de Spearman (rS) entre os escores obtidos para o DS5 e cada um dos processos de três domínios do COBIT estão apresentados na tabela 1. O coeficiente de Spearman foi também calculado porque, para dados em escala de Likert, a pressuposição de normalidade nem sempre é satisfeita. Observou-se, no entanto, que em todas as variáveis, a diferença entre os coeficientes "r" e "rS" foi mínima, na ordem de 0,01. Decidiu-se, então, seguir com as análises deixando de lado as técnicas não paramétricas.

Processo	r Pearson	rS Spearman
Planejamento e organização:		
PO1 - Define o planejamento estratégico de TI.	0.439	0.428
PO2 - Define a arquitetura da informação.	0.449	0.459
PO3 - Determina as diretrizes da Tecnologia.	0.480	0.466
PO4 - Define a organização de TI e seus relacionamentos.	0.432	0.421
PO5 - Gerencia o investimento de TI.	0.519	0.518
PO6 - Comunica as metas e diretrizes gerenciais.	0.306	0.311
PO7 - Gerencia os RH de TI.	0.311	0.313
PO8 - Gerencia a qualidade.	0.284	0.288
PO9 - Avalia e gerencia os riscos.	0.408	0.402
PO10 - Gerencia os projetos.	0.411	0.405
Aquisição e implementação:		
AI1 - Identifica soluções de automação.	0.409	0.407
AI2 - Adquiri e mantém *software* aplicativo.	0.416	0.422
AI3 - Adquire e mantém a arquitetura tecnológica.	0.535	0.529
AI4 - Desenvolve e mantém procedimentos de TI.	0.467	0.480
AI5 - Obtém recursos de TI.	0.590	0.581

Processo	r Pearson	rS Spearman
AI6 - Gerenciar mudanças	0.455	0.457
AI7 - Instala e certifica soluções e mudanças.	0.469	0.458
Monitoramento:		
MO1 - Monitora e avalia a desempenho de TI.	0.437	0.440
MO2 - Monitora e avalia o controle interno.	0.465	0.461
MO3 - Assegura a conformidade aos requisitos externos.	0.449	0.443
MO4 - Fornecer governança de TI.	0.439	0.428

[1] Todos os coeficientes são estatisticamente significativos (P < 0,001)

Tabela 2 – Coeficientes de correlação linear de Pearson (r) e não-paramétrico de Spearman (rS) [1] entre os escores de DS5 e cada um dos escores dos processos de três domínios do COBIT, em microempresas e empresas de pequeno e médio porte (N = 180)

As correlações entre DS5 e os demais processos foram todas estatisticamente significativas (P <0,001), com valores que mostraram alguma variação dentro do mesmo domínio. No domínio Planejamento e Organização (PO), os coeficientes de oscilaram entre 0,28 (PO8) e 0,52 (PO5), em Aquisição e Implementação (AI) variaram entre 0,41 (AI1 e AI2) e 0,59 (AI5) e no domínio de Monitoramento (MO) ficaram entre 0,44 e 0,46.

As maiores correlações ("r" acima de 0,47) com DS5 ocorreram, no domínio PO, com os processos PO3 e PO5, enquanto no domínio Aquisição e Implementação (AI) foram com os processos AI5, AI4 e AI7. No domínio de Monitoramento (MO), as correlações foram 0,44, com uma exceção (MO2 = 0,46). Como seria de se esperar, em cada domínio os escores dos processos tecnológicos estão correlacionados entre si.

Considerando que os processos estão correlacionados, a pergunta é: haverá algum que impacta mais, se considerarmos a correlação entre eles? A análise de regressão linear múltipla foi usada para avaliar o efeito individual de cada processo, ajustando pela correlação que ele tem com os demais processos do domínio. Foram realizadas três análises, uma para cada domínio de processos.

A Tabela 3 apresenta os resultados da regressão múltipla para o domínio Planejamento e Organização (PO).

Devido à correlação interna (multicolinearidade) entre os processos de PO, quando se analisar todos os processos juntos a significância estatística da relação de 8 processos com DS5 se perde. Assim se vê que quando se ajusta pelos demais processos, PO5 - Gerencia o investimento em TI é o processo que mais está associado a DS5 (b=0,32; P=0,001). O processo PO6 - Comunica as metas e diretrizes gerenciais também tem relação com DS5, mas se ajustado pelo efeito dos demais processos, a relação é negativa (b=-0,27; P=0,014).

Processos de Planejamento e Organização	B ajustado	P
PO1 - Define o planejamento estratégico de TI.	0,105	0,432
PO2 - Define a arquitetura da informação.	0,136	0,272
PO3 - Determina as diretrizes da tecnologia.	0,099	0,411
PO4 - Define a organização de TI e seus relacionamentos.	0,127	0,158
PO5 - Gerencia o investimento de TI.	0,317	0,001
PO6 - Comunica as metas e diretrizes gerenciais.	-0,268	0,014
PO7 - Gerencia os recursos humanos de TI.	0,110	0,282
PO8 - Gerencia a qualidade.	-0,146	0,123
PO9 - Avalia e gerencia os riscos.	0,157	0,125
PO10 - Gerencia os projetos.	0,098	0,313

Tabela 3 – Regressão múltipla de DS5 em relação aos processos do domínio Planejamento e Organização (PO): coeficientes de regressão ajustados e valores-P

O resultado relativo a PO5 já podia ser antecipado pala análise de correlação simples (Tabela1), mas o efeito de PO6 é um resultado novo, que reflete a importância de considerar a correlação entre variáveis do mesmo domínio. Os coeficientes obtidos na regressão múltipla entre os escores do domínio AI e o processo DS5 está apresentado na Tabela 4.

Processos de Aquisição e Implementação	B ajustado	P
AI1 - Identifica soluções de automação.	-0,063	0,507
AI2 - Adquiri e mantém *software* aplicativo.	0,051	0,565
AI3 - Adquire e mantém a arquitetura tecnológica.	0,194	0,038
AI4 - Desenvolve e mantém procedimentos de TI.	0,026	0,791
AI5 - Obtém recursos de TI.	0,357	<0,001
AI6 - Gerenciar mudanças	0,083	0,338
AI7 - Instala e certifica soluções e mudanças.	0,129	0,131

Tabela 4 – Regressão múltipla de DS5 em relação aos processos do domínio Análise e Implementação (AI): coeficientes de regressão ajustados e valores-P

Na análise de correlação simples, todos os sete processos estavam correlacionados com os valores do processo DS5. As correlações internas entre os processos do domínio AI variaram entre 0,495 e 0,649. Assim, embora nas análises individuais todos os processos estivessem associados ao DS5, quando avaliados em conjunto se vê que AI5 - Obtém recursos de TI é o processo que está mais associado estatisticamente aos escore de DS5 (P<0,001).

O processo AI3 - Adquire e mantém a arquitetura tecnológica, também foi estatisticamente significativo ajustando pelos escores dos demais processos. AI3 tem relação com DS5 em

menor grau (o aumento esperado em DS5 é de 0,19 para cada escore a mais em AI3; p=0,038) do que AI5 (b=0,36).

Para o domínio Monitoramento (MO) de processos, os resultados da regressão múltipla podem ser encontrados na Tabela 5.

Processos de Monitoramento	B ajustado	P
MO1 - Monitora e avalia a desempenho de TI.	0,146	0,111
MO2 - Monitora e avalia o controle interno.	0,196	0,056
MO3 - Assegura a conformidade aos requisitos externos.	0,199	0,016
MO4 - Fornecer governança de TI.	0,139	0,129

Tabela 5 – Regressão múltipla de DS5 em relação aos processos do domínio Monitoramento (MO): coeficientes de regressão ajustados e valores-P

Os processos do domínio Monitoramento apresentaram coeficientes de correlação intradomínio que variaram entre 0,482 e 0,659. Quando analisados em conjunto, o processo MO3 - Assegura a conformidade aos requisitos externos foi único que, quando ajustado pelos demais processos do domínio, apresentou associação estatisticamente significativa com DS5. A associação foi fraca, representando um aumento de 0,20 no escore de DS5 para cada aumento de uma unidade em MO3. Resultado semelhante, mas não significativo estatisticamente, foi observado para MO2.

A partir dos resultados obtidos para os três domínios, surgiu a seguinte a pergunta: se considerarmos, como representante de cada domínio, a variável que teve maior efeito sobre DS5, e analisarmos as três em conjunto, qual domínio teria maior associação com DS5? O resultado da análise de regressão múltipla com os preditores PO5, AI5 e MO# estão apresentados na Tabela 6.

Processos	B ajustado	P
PO5 - Gerencia o investimento de TI.	0,246	0,002
AI5 - Obtém recursos de TI	0,393	<0,001
MO3 - Assegura a conformidade aos requisitos externos.	0,195	0,003

Tabela 6 – Regressão múltipla dos escores de DS5 sobre os processos que mais impactaram seu valor nos três domínios

Quando se ajusta pelos demais processos presentes no modelo, AI5 – Obtém recursos de TI é o processo que mais afeta DS5 (b ajustado = 0,39), enquanto os coeficientes b dos outros processos ficaram abaixo de 0,25. Este resultado foi conferido por uma análise de componentes principais que mostrou que o domínio AI é o que está mais associado aos valores de DS5.

5. Conclusões

Este trabalho objetivou analisar processos tecnológicos para aumento das garantias de segurança de sistemas, representada pelo processo DS5 (Garantir segurança dos

sistemas) usando análise de correlação e regressão linear simples e múltipla. Com isso pôde-se compreender com a contribuição empírica desde estudo que no grupo das micro, pequenas e médias empresas industriais do sul do Brasil os processos PO5 (Gerenciar o investimento de TI), do domínio de Planejamento e Organização (PO), AI5 (Obtém recursos de TI) do domínio de Aquisição e Implementação, e MO3 (Assegura a conformidade aos requisitos externos), do domínio de Monitoramento (MO) são os que têm mais impacto sobre DS5 quando confrontados com os demais processos do seu respectivo domínio. Quando se analisa estes três processos juntos, se nota que o domínio AI (Obtém recursos de TI) é o que se sobressai em termos de influência sobre DS5.

As contribuições teóricas estão diretamente relacionadas a uma abordagem estratégica na qual são estabelecidas questões prioritárias para o planejamento empresarial, interconectadas com o ambiente operacional e com impacto no retorno sobre o investimento. Este estudo contribui para a gestão do investimento em recursos tecnológicos, gestão do comportamento dos funcionários, cultura organizacional e questões relacionadas com a consciência estratégica dos recursos humanos para desenvolver abordagens e práticas alinhadas com os objetivos organizacionais.

Para estudos futuros, se propõem aqui ampliar as análises para integrar as técnicas de estatística com as de mineração de dados e inteligência artificial. Assim cada vez que a empresa audita seus processos, sejam eles corporativos ou tecnológicos, essas técnicas podem automaticamente corrigir eventuais distorções. Também é sugerido desenvolver projetos entre países para analisar esses mesmos impactos de processos tecnológicos na segurança de sistemas e na estratégia de negócios e de TI, bem como aprimorar ainda mais os níveis de maturidades empresarial.

Agradecimentos

Queremos agradecer ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) do Ministério da Ciência, Tecnologia e Inovação do Brasil pelo apoio recebido através do Projeto CNPq/Universal 7764933922392857.

Referencias

Aguiar, J., Pereira, R., Vasconcelos, J., & Bianchi, I. (2018). Na overlapless incident management maturity model for multi-framework assessment (ITIL, COBIT, CMMI-SVC). *Interdisciplinary Journal of Information, Knowledge, and Management*, *13*, 137-163. https://doi.org/10.28945/4083

Alkhaldi, F., Hammami, S., & Uddin, M. A. (2017). Understating value characteristics toward a robust IT governance application in private organizations using COBIT framework. *International Journal of Engineering Business Management*, *9*(1), 1-8. https://doi.org/10.1177/1847979017703779

Argyris, C. (1996). Toward a comprehensive theory of management. In: Edmondson, A.; Moingeon, B. (Eds.), *Organizational learning and competitive advantage*. London: Sage.

Bernard, P. (2012). *COBIT® 5 – A Management Guide*. Amersfoort, NL: Van Haren Publishing.

Beyer, J., & Trice, H. (1987) How an organization's rites reveal its culture. *Organizational Dynamics*, *15*(4), 5-24. https://doi.org/10.1016/0090-2616(87)90041-6

Bonabeau, E. (2002). Predicting the unpredictable. *Harvard Business Review*, *80*(3), 109-116.

Buccafurri, F., Fotia, L., Furfaro, A., Garro, A., Giacalone, M., & Tundis, A. (2015). An analytical processing approach to supporting cyber security compliance assessment. *Proceedings of the 8th International Conference on Security of Information and Networks*, 46-53.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know*. Boston: Harvard Business School Press.

Debreceny, R., & Gray, G. (2013). IT governance and process maturity: a multinational field study. *Journal of Information Systems*, *27*(1), 157-188. https://doi.org/10.2308/isys-50418.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125-128.

Europol (2020). How COVID-19-related crime infected Europe during 2020. https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020. Acesso em 12 janeiro 2021.

Farazzmanesh, F., & Hosseini, M. (2017). Analysis of business customers' value network using data mining techniques. *Journal of Information Systems and Telecommunication, 5*(3), 162-171.

Gao, F., Rau, P. L. P., & Zhang, Y. (2018). Perceived mobile information security and adoption of mobile payment services in China. In *Mobile commerce: Concepts, methodologies, tools, and applications*. USA: IGI Global.

Gerl, A., von der Heyde, M., Groß, R., Seck, R., & Watkowski, L. (2021). Applying COBIT 2019 to IT Governance in Higher Education. In: Reussner, R. H., Koziolek, A. & Heinrich, R. (Hrsg.), INFORMATIK 2020. Gesellschaft für Informatik, Bonn. (S. 517-530). https://doi.org/10.18420/inf2020_47

Gleiser, I. (2002). *Caos e Complexidade: a evolução do pensamento econômico*. RJ: Campus.

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, *181*, 59-66. https://doi.org/10.1016/j.procs.2021.01.103

Hadlington, L., Binder, J., & Stanulewicz, N. (2021). Exploring role of moral disengagement and counterproductive work behaviours in information security awareness. *Computers in Human Behavior, 114*, 106557. https://doi.org/10.1016/j.chb.2020.106557

Hofstede, G. (1984). *Culture´s consequences: international differences in work-related values*. London: Sage Publications.

Information Technology Governance Institute - ITGI (2003). *Board briefing on IT governance*. 2nd ed. IL: IT Governance Institute.

Information Technology Governance Institute - ITGI (2007). *CobiT 4.1: Framework, control objectives, management guidelines, maturity models*. IL, USA: IT Governance Institute.

Instituto Brasileiro de Governança Corporativa - IBGC (2015). *Código das melhores práticas de governança corporativa*. 5ª. ed. São Paulo: IBGC.

Instituto Brasileiro de Governança Corporativa - IBGC (2020). *O que é governança corporativa*. São Paulo: IBGC.

ISACA (2012). *COBIT 5 – Modelo corporativo para governança e gestão de TI da organização*. Rolling Meadows, IL: ISACA.

ISACA (2018). *What is COBIT 5?* Rolling Meadows, IL: ISACA.

ISACA (2021). *Design guide and toolkit*. *Designing an information & technology governance solution*. Rolling Meadows, IL: ISACA

ISO/IEC 27002: 2007. Tecnologia da Informação – Código de prática para a gestão da segurança da informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas.

ISO/IEC 27032: 2012. Information technology: Security techniques: Guidelines for cybersecurity. Geneva: International Organization for Standardization.

Justitiaa, A., Zaman, B., & Putra, D. (2021). Evaluating the quality of a help-desk complaint management service using six-sigma and COBIT 5 framework. *AIP Conference Proceedings*. 2329, 050009. https://doi.org/10.1063/5.0042166

Kaplan, R. S., & Norton, D. P. (2004). *Strategy maps: Converting intangible assets into tangible outcomes*. USA: Harvard Business School Press.

Klir, G. J., Clair, U. H. S., & Yuan, B. (1997). *Fuzzy Set Theory: Foundations and Applications*. London: Prentice-Hall.

Malatji, M., Marnewick, A. L., & Von Solms, S. (2021). Cybersecurity capabilities for critical infrastructure resilience. *Information and Computer Security*, ahead-of-print. https://doi.org/10.1108/ICS-06-2021-0091

Mintzberg, H. (1994). *The rise and fall of strategic planning*. New York: Free Press.

Mintzberg, H., Ahlstrand, B., & Lampel, J. (1998). *Strategy safari: A guided tour through the wilds of strategic management*. New York: Prentice-Hall.

Morgan, G. (1986). *Images of Organization*. London: Sage.

Morin, E. (2003). *Introdução ao pensamento complexo*. 4 ed. Lisboa: Instituto Piaget.

OECD (2018). *G20/OECD principles of corporate governance*. Paris, France: OECD Publishing. https://doi.org/10.1787/9789264236882-en

Peters, T., & Waterman, R. (1982): *In Search of Excellence: Lessons from America´s best-run companies*. USA: Haper Business.

Porter, M. (1990). *Vantagem competitiva*: *criando e sustentando um desempenho superior*. Rio de Janeiro: Campus.

Prahalad, C. K., & Hamel, G. (1990). The core competence of the corporation. *Harvard Business Review*, *68*(3), 79-91.

Raisinghani, M. S. (2000). Knowledge management: A cognitive perspective on business na deducation. *American Business Review, 18*(2), 105-112.

Rohn, E., Sabari, G., & Leshem, G. (2016). Explaining small business InfoSec posture using social theories. *Information and Computer Security*, *24*(5), 534-556. https://doi.org/10.1108/ICS-09-2015-0041

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82. https://doi.org/10.1016/j.cose.2015.10.006

Schein, E. (1992). *Organizational Culture and Leadership*. San Francisco: Josey-Bass.

Shamala, P., Ahmad, R., Zolait, A. H., & bin Sahib, S. (2015). Collective information structure model for Information Security Risk Assessment (ISRA*). Journal of Systems and Information Technology*, *17*(2), 193-219. https://doi.org/10.1108/JSIT-02-2015-0013

Simon, H. A. (1961). *Administrative behavior*. 2nd ed. New York: Macmillan.

Simon, H. A. (1996). *The sciences of the artificial*. 3rd ed. Cambridge: MIT Press.

Slayton, R. (2021). Governing uncertainty or uncertain governance? Information security and the challenge of cutting ties. *Science, Technology, & Human Values*. *46*(1), 81-111. https://doi.org/10.1177/0162243919901159

Spears, J. L., & Barki, H. (2010) User participation in information systems security risk management. *MIS Quarterly*, *34*(3), 503-522. doi: 10.2307/25750689

Trice, H., & Beyer, J. (1984). Studing organizational cultures through rites and ceremonials. *The Academy of Management Review*, *9*(4), 653-669. https://doi.org/10.2307/258488

Weill, P., & Ross, J. W. (2005). *IT governance: How top performers manage IT decision rights*. USA: Harvard *Business Review Press*.

Wilkin, C., & Chenhall, T. (2010). A review of IT governance: A taxonomy to inform accounting information systems. *Journal of Information Systems*, *24*(2), 107-146. https://doi.org/10.2308/isys-50922

Wrigh, P., Kroll, M. J., & Parnell, J. A. (1998). *Strategic management: concepts and cases*. New Jersey: Prentice Hall.

Young, R. F., & Windsor J. (2010) Empirical evaluation of information security planning and integration. *Communications of the Association for Information Systems*, *26*(13), 245-266. https://doi.org/10.17705/1CAIS.02613

Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, *8*(3), 338-353. https://doi.org/10.1016/S0019-9958(65)90241-X