AVALIAÇÃO DE UMA EMPRESA DE TECNOLOGIA ATRAVÉS DE ALGUNS CONTROLES DA NBR ISO/IEC 27001/2013 DIRECIONADOS AOS RECURSOS HUMANOS

EVALUATION OF A TECHNOLOGY COMPANY THROUGH SOME CONTROLS OF NBR ISO/IEC 27001/2013 DIRECTED TO HUMAN RESOURCES

Francisco Américo da Silva, Fatec Americana, francisco.silva102@fatec.sp.gov.br
Edson Roberto Gaseta, Fatec Americana, edson.gaseta01@fatec.sp.gov.br

Resumo

Este trabalho explora o tema Segurança da Informação (SI) no contexto do departamento de Recursos Humanos (RH) de uma empresa de tecnologia, e tem por objetivo avaliar os processos desse departamento pautados por alguns controles da norma NBR ISO/IEC 27001/2013. Para tanto, buscou-se através de revisão de literatura alicerçar os principais conceitos relacionados a SI e a evolução do RH com intuito de evidenciar com pesquisa de campo como os controles demonstrados pela academia, e pelo mercado (framework NBR ISO/IEC 27001/2013), são executados na prática pela empresa. As evidências ganham um aspecto concreto com a utilização das métricas do nível de maturidade do COBIT, que aliado à norma NBR ISO/IEC 27001/2013 se mostra uma excelente ferramenta para viabilizar o estudo. A pesquisa conclui que a empresa atinge um bom nível de maturidade dos controles em decorrência do tipo de trabalho realizado e da recente adequação de seus processos para atender a Lei Geral de Proteção de Dados (LGPD).

Palavras-chave: auditoria em sistemas de informações, segurança da informação no RH, estudo de caso.

Abstract

This work explores the Information Security (IS) subject in the context of the Human Resources (HR) department of a technology company. It aims to evaluate the processes of this department guided by some controls of the NBR ISO/IEC 27001/2013 standard. To this end, it sought, through a literature review, to base the main concepts related to IS and the evolution of HR to demonstrate with field research how the controls shown by the academy and by the market (framework NBR ISO/IEC 27001/2013), are executions in practice by the company. As proven, it gains a concrete aspect with the use of COBIT maturity level metrics, which, combined with the NBR ISO/IEC 27001/2013 standard, proves to be an excellent tool to make the study feasible. The research concludes that the company reached a good level of maturity of the controls due to the type of work carried out and the recent updates of its processes to comply with the Lei Geral de Proteção de Dados (LGPD).

***Keywords**: information systems audit, information security in HR, case study.*

1. Introdução

O tema de Segurança da Informação (SI) tem se tornado cada vez mais presente na vida das pessoas e das organizações, seja no que diz respeito à proteção de seus dispositivos pessoais ou na proteção dos ativos das empresas, ou ainda na leitura de reportagens sobre novas regulamentações como a Lei Geral de Proteção de Dados (LGPD).

Nesse cenário, o presente estudo se concentra na exploração SI, com enfoque no Departamento de Recursos Humanos (RH), uma tarefa que envolve tanto empresas como pessoas.

A princípio a revisão de literatura esclarece o conceito de SI, e explica como ocorreu a evolução do Departamento Pessoal (DP) para o Departamento de Recursos Humanos (RH). Em seguida, traz a discussão a NBR ISO/IEC 27001/2013 uma importante Norma para desenvolver um Sistema de Gestão de Segurança da Informação (SGSI), e adiante elucida como esta questão envolve o departamento de RH e os demais níveis organizacionais dentro das empresas.

A pergunta-problema que segue o desenvolvimento deste projeto é “como avaliar o Departamento de Recursos Humanos (RH) de uma empresa de tecnologia da cidade de Piracicaba/SP em relação a Segurança da Informação (SI) com base em alguns controles da norma NBR ISO/IEC 27001/2013”.

Os objetivos específicos são realizar uma pesquisa bibliográfica sobre Segurança da Informação (SI) aplicada ao departamento de Recursos Humanos (RH) e coletar dados por meio de questionário aplicado ao departamento estudado.

Trata-se de um estudo importante para a academia e para o pesquisador, pois para um é uma forma de relacionar os conhecimentos adquiridos em sala de aula com um projeto aplicado, e para o outro é a união de dois temas interessantes Segurança da Informação e Recursos Humanos.

2. Referencial Teórico

A revisão de literatura apresentada tem o intuito de formar um panorama geral da Segurança da Informação (SI), apresentar o departamento de Recursos Humanos (RH) e

comentar sobre sua importância nas organizações, introduzir a ISO 27001:2013 uma das normas de referência da área de gestão de segurança, e por fim esclarecer conceitos chaves que acompanham o desenvolvimento deste estudo.

2.1. Segurança da Informação

A Segurança da Informação (SI) possui significados distintos para diferentes grupos, como por exemplo, para fornecedores de soluções de segurança, o conceito está relacionado aos equipamentos que vendem e fortalecem a segurança da tecnologia da informação, já para os diretores pode ser algo difícil de compreender e que o departamento de tecnologia precisa lidar, e por fim para os usuários geralmente são os bloqueios que os impedem de acessar *websites* e instalar *softwares* nos computadores da empresa (CALDER e WATKINS, 2020).

Essas tentativas de definições possuem enfoques estreitos, pois os fornecedores, diretores e usuários do exemplo associam o significado da SI às situações que estão próximas às suas atividades diárias. Portanto, não visualizam com plenitude a real importância do tema.

Para um especialista a SI está relacionada à capacidade de preservar o valor das informações das pessoas ou organizações, de tal forma que visa protegê-las contra as diversas ameaças a que estão expostas, avaliar riscos, e promover a continuidade dos negócios (FERREIRA, 2017).

Com efeito, definir SI e seus termos relacionados é de fundamental importância para compreensão deste assunto, sendo assim, existe uma norma específica com intuito de fornecer esses esclarecimentos.

A Organização Internacional para Padronização (ISO) é uma entidade com sede em Genebra que desenvolve normas técnicas para padronização e normatização, e no que se relaciona a SI a ISO desenvolveu a norma técnica ISO/IEC 27000:2018 que é a raiz de uma série de padrões internacionais que fornecem uma visão geral dos Sistemas de Gerenciamento de Segurança da Informação (SGSI), além dos termos e principais definições que são utilizadas em todas as normas dessa família (CALDER e WATKINS, 2020).

Para a ISO a SI é a “preservação da confidencialidade, integridade e

disponibilidade das informações" (ISO, 2018, p.4, tradução nossa), e somente é alcançada quando há implementação de um conjunto de controles que são selecionados através da avaliação de riscos para que possam ser gerenciados por meio de um SGSI, isto inclui o desenvolvimento de políticas, processos, procedimentos, *softwares* e *hardwares* para proteção dos ativos em relação aos riscos identificados (ISO, 2018).

Em suma, a SI tem importância tanto para as pessoas quanto para as organizações, nesse sentido, as pessoas como consumidoras necessitam que seus dados sejam íntegros quando realizam uma compra, e que o comprovante seja emitido e, portanto, esteja disponível para sua visualização, além de ser confidencial. Já na perspectiva das organizações, elas possuem dados ou informações importantes que gostariam de proteger, uma vez que são através do processamento desses dados e informações que são geradas as vantagens competitivas.

2.2. Recursos Humanos

O Departamento de Recursos Humanos (RH) é um dos departamentos mais importantes dentro da organização como certa vez declarou Walt Disney "você pode sonhar, projetar, criar e construir o lugar mais maravilhoso do mundo, mas é preciso pessoas para tornar o sonho realidade" (NADER, 2014, p. 169, *apud* ELIA, 2021, p. 2).

Nesse sentido, o RH (como também é conhecido) acompanha a evolução das organizações desde a Revolução Industrial, movimento iniciado na Inglaterra no fim do século XVIII, que foi significativo devido à utilização das primeiras máquinas movidas a vapor para transporte e produção (SCHREINER e BUSANELLO, 2018).

No período as primeiras fábricas criaram um cenário que permitia a entrega de grandes quantidades de produtos, e isso gerou a necessidade de mais pessoas trabalhando. Consequentemente surgiu o Departamento Pessoal (DP), que na realidade era o próprio dono do negócio, e tinha a incumbência de controlar horas trabalhadas *versus* pagamentos (ELIA, 2021).

A seguir com a intensificação da produção, e a partir da metade do século XIX ocorre a Segunda Revolução Industrial, movimento global, pois já haviam outros países industrializados nesse período, e o ponto principal foi à introdução do petróleo como fonte de energia, a utilização da energia elétrica, invenção do automóvel e telefone (SCHREINER e BUSANELLO, 2018).

Observa-se que as indústrias foram crescendo e mais pessoas foram necessárias para suportar esse crescimento, nesse sentido o DP também mudou, e ao assumir outros subsistemas como recrutamento e seleção, treinamento e desenvolvimento, cargos e salários, folha de pagamento, benefícios e entre outros passou a ser conhecido como departamento de Recursos Humanos (RH) ou Gestão de Pessoas (GP) (RIBEIRO, 2017).

Por conseguinte quanto mais subsistemas esta área incorpora, mais é a quantidade de dados e informações que passa a agregar, em vista disso olhar a gestão de pessoas com a lente da segurança da informação se demonstra necessário.

2.3. NBR ISO/IEC 27001/2013

A Associação Brasileira de Normas Técnicas (ABNT) é uma entidade privada, sem fins lucrativos responsável pela elaboração das Normas ABNT NBR a partir de seus subcomitês que atuam em parceria com governos e a sociedade para implementação de políticas públicas, desenvolvimento de mercados e defesa dos consumidores (ABNT, 2022).

Em relação à segurança da informação a ABNT produziu a NBR ISO/IEC 27001/2013, que possui a mesma nomenclatura da versão internacional acrescentado o NBR, para estabelecer, implementar, manter e melhorar um sistema de segurança da informação (ABNT, 2013).

A ISO/IEC 27001/2013: “Information technology - Security techniques - Information security management systems - Requirements” a qual originou a norma brasileira é um padrão internacional que não é obrigatório para as empresas ou setores específicos, todavia é bem conhecido e utilizado amplamente (LANDOLL, 2016).

Sendo assim a norma está organizada em sete seções nas quais referenciam 114 controles em 14 grupos, de modo que as cláusulas são de alto nível, ou seja, requerem a interpretação e não especificam como desenvolver políticas, procedimentos e processos que compõe o sistema de gestão da segurança da informação (LANDOLL, 2016).

A organização que trabalha os requisitos propostos nas sete seções, sendo eles *i.* contexto da organização, *ii.* liderança, *iii.* planejamento, *iv.* apoio, *v.* operação, *vi.* avaliação do desempenho e *vii.* melhoria está apta para obter uma certificação que sinaliza que possui conformidade com a ISO 27001 (SUDOSKI, 2017).

Dos 14 grupos que são referenciados no Anexo A da NBR ISO/IEC 27001/2013 que abrangem a segurança em todos os aspectos da organização, o grupo A.7 Segurança em recursos humanos é de fundamental importância para este estudo, e a seção seguinte tem o intuito de aprofundar a revisão de literatura.

2.4. Segurança em Recursos Humanos

Conforme apresentação da Figura 1, a segurança em recursos humanos são abordadas sob três perspectivas, sendo: *i.* antes da contratação, *ii.* durante a contratação e *iii*. encerramento e mudança da contratação.

Figura 1 - Grupos de controle de segurança em RH da ISO

GRUPOS	OBJETIVOS	
A.7 Segurança em recursos humanos	A.7.1 Antes da contratação	Assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.
	A.7.2 Durante a contratação	Assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação.
	A.7.3 Encerramento e mudança da contratação	Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.

Fonte: adaptado ABNT, 2013

Com o conhecimento da norma que é abordada nesta seção, pode-se introduzir a premissa que considera as pessoas como parte dos ativos da organização. De acordo com Smulders *et al*. (2018) as pessoas, conhecimentos e habilidades que possuem compõem parte da empresa, e, portanto, necessitam de atenção em relação a segurança da informação.

A norma deixa evidente que todos os funcionários são responsáveis pela SI, e ainda se pode ressaltar que é de suma importância o desenvolvimento de procedimentos para contratação, mudança ou desligamento de funcionários da empresa, mas não limitado aos colaboradores diretos, sendo, deste modo, as mesmas responsabilidades estendidas para contratos terceirizados (CALDER e WATKINS, 2020).

O controle 7.1 da norma e subsequentes abordam o período antes da contratação, e neste caso tem o intuito de garantir que os funcionários e partes externas entendem suas responsabilidades em relação a SI. É evidente que se trata de um processo pré-triagem, no qual enseja verificar informações de cunho pessoal e profissional como a exatidão do currículo, informações acadêmicas e profissionais, verificação de identidade e registros criminais (SMULDERS *et al.*, 2018). Calder e Watkins (2020) recomendam nessa fase

ter uma descrição das competências exigidas para o cargo, e em especial detalhada para os que compõem o sistema de gestão de segurança da informação. Neste contexto, quanto mais informações confidenciais e de alta sensibilidade o futuro funcionário tiver acesso, mais rigorosa deve ser a verificação na qual lhe será submetida.

Calder e Watkins (2020) argumentam que é importante descrever no contrato de trabalho que o funcionário é responsável pela SI, ou alternativamente mencionar no contrato uma referência a política de segurança da informação. Além das responsabilidades em relação a qualquer legislação vigente que possa afetar a confidencialidade, integridade, e disponibilidade das informações durante o vínculo de emprego ou mesmo após seu encerramento.

Para consolidar a discussão referente às leis, a Lei Geral de Proteção de Dados (LGPD) deve ser mencionada no contrato de trabalho, haja vista que causa impactos significativos às organizações em relação ao seu descumprimento. Não obstante, algumas leis específicas podem ser consideradas importantes referenciar como a Lei de Propriedade Industrial (Lei 9.279/1996), a Lei de Direitos Autorais (Lei 9.610/1998) e a Lei de Softwares (Lei 9.609/1998) (BORELLI, GUTIERREZ, *et al.*, 2019).

Embora pareça muita informação para o processo de entrada de funcionários na empresa, o consultor Volchkov (2018) sinaliza que promover conhecimento sobre a estrutura legal e regulatória que a empresa está incluída a protege contra possíveis sanções, e permite aos funcionários compreensão dos impactos de suas ações no trabalho.

O próximo controle macro descrito na norma é o 7.2 durante o emprego que tem por objetivo assegurar que os funcionários e partes externas estejam conscientes e cumpram as responsabilidades em relação à segurança da informação.

Nesse contexto conforme Smulders *et al.* (2018) é necessário trabalhar no treinamento de integração o tema SI, bem como entregar aos funcionários folhetos, e boletins informativos, vídeos e cartazes. De acordo com o público-alvo, materiais diferentes devem ser elaborados, assim como treinamentos distintos para as diferentes funções dentro da organização.

Com a proposta de capacitação, Calder e Watkins (2020) agregam que promover a conscientização através do método de *e-learning* (ensino com suporte das tecnologias da informação) tem mais efeito do que reunir funcionários em uma sala de reunião para

transmitir o conteúdo. A vantagem do *e-learning* é conceder flexibilidade, bem como introduzir materiais como vídeos, fotos e textos.

Ainda nesse cenário, mesmo com a adoção de práticas de conscientização dos funcionários, há necessidade de se pensar que desvios podem ocorrer, e, portanto, a ABNT (2013) traz um controle específico para os processos disciplinares que deve ser informado no contrato de trabalho, e como Smulders *et al.* (2018) propõem a divulgação nos treinamentos, já que as violações precisam ser acompanhadas por um processo disciplinar conhecido.

O último controle macro da norma é o 7.3 encerramento e mudança da contratação cujo objetivo é proteger os interesses da empresa quando ocorre um processo de término de contrato ou alteração de função.

Para atender esse requisito é necessário observar vários aspectos que são cobertos pela ISO/IEC 27001/2013 como devolução dos equipamentos da empresa, remoção ou ajuste de direitos de acessos (ABNT, 2013). Na visão de Calder e Watkins (2020), a rescisão de contrato de trabalho é muitas vezes conduzida de modo inadequado e isso cria novas vulnerabilidades que precisam ser avaliadas adequadamente. Na mesma linha de pensamento os autores Smulders *et al.* (2018) argumentam que mesmo com o encerramento do contrato, algumas responsabilidades continuam existindo, portanto, ter assinado previamente um termo de confidencialidade, é de vital importância para que seja lembrado ao ex-funcionário sobre essas responsabilidades.

Em resumo são diversos os aspectos relacionados a SI que envolve o departamento RH, e embora a norma pontue três momentos da gestão do funcionário dentro da organização, sendo antes da contratação, durante o contrato e término do vínculo empregatício, pode-se visualizar que muitos dos itens mencionados trazem uma bagagem de outras seções.

2.5. Controles Relacionados ao RH

No Quadro 3 são apresentados alguns controles importantes relacionados à temática do estudo, e que são necessários para a compreensão da totalidade da segurança da informação no departamento de RH.

Figura 2 - Controles de segurança adicionais para RH extraídos de outras seções da ISO

GRUPOS	OBJETIVOS	
A.5 Políticas da segurança da informação	A.5.1 Orientação da direção para segurança da informação	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.
A.6 Organização da segurança da informação	A.6.2 Dispositivos móveis e trabalho remoto	Garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis.
A.9 Controle de acesso	A.9.1 Requisitos do negócio para controle de acesso	Limitar o acesso à informação e aos recursos de processamento da informação.
	A.9.2 Gerenciamento de acesso do usuário	Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.
A.18 Conformidade	A.18.1 Conformidade com requisitos legais e contratuais	Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas a segurança da informação e de quaisquer requisitos de segurança.

Fonte: adaptado ABNT, 2013

O grupo de controle A.5 Políticas de segurança da informação evidencia o controle A.5.1 Orientação da direção para segurança da informação que possui o objetivo de direcionar a empresa sobre o que é esperado dos departamentos e funcionários em relação à segurança da informação. Nesse sentido, a política de segurança da informação é o principal documento do SGSI, uma vez que reflete a visão da alta administração (nível estratégico) em relação a SI com base nos objetivos estratégicos de negócio, as limitações da empresa e oportunidades percebidas (CALDER e WATKINS, 2020).

No grupo de controle A.6 Organização da segurança da informação o controle A.6.2 Dispositivos móveis e trabalho remoto se tornou necessário para muitas empresas com a pandemia de 2019 quando o governo declarou a quarentena para enfrentar o estado de emergência de saúde pública de importância internacional decorrente do coronavírus. Na época o *home office* foi a solução adotada para manter as operações tanto nas grandes quanto nas médias empresas (MELLO, 2020, on-line).

Com este contexto, é impreterível adotar uma política de trabalho remoto, uma vez que as medidas de proteção disponíveis dentro da organização não alcançam os ambientes de trabalhos externos como a residência do funcionário (SMULDERS, BAARS, *et al.*, 2018). Sendo assim, ao adotar o trabalho remoto há necessidade de procedimentos que incluam autorização, provisão de equipamentos, segurança da informação durante o trabalho remoto, e uso do equipamento de trabalho remoto (CALDER e WATKINS, 2020).

O grupo A.9 Controle de acesso são dois os controles particularmente importantes para este estudo, sendo A.9.1 Requisitos do negócio para controle de acesso e A.9.2 Gerenciamento de acesso do usuário. Com visão macro se pode entender que o funcionário deve ter acesso suficiente para executar as tarefas que são de sua alçada, e, portanto, não deve ser capaz de acessar informações que não fazem parte do seu escopo de trabalho (CALDER e WATKINS, 2020).

No último grupo de controle identificado para este estudo o A.18 Conformidade, especificamente o controle A.18.1 Conformidade com requisitos legais e contratuais tem o objetivo assegurar que a empresa não deixe de cumprir qualquer lei, obrigação, regulamentação ou contrato que esteja vinculado a sua atividade. Na visão de Calder e Watkins (2020) a empresa deve definir e documentar todos os requisitos relacionados aos sistemas de informação que possui e inclusive manter atualizado os controles específicos e responsabilidades individuais.

Nesta seção foram apresentados alguns controles que estão em outras seções da norma ABNT ISO/IEC 27001/2013, e são relevantes para o desenvolvimento dos trabalhos no departamento de RH.

3. Metodologia

O presente estudo é caracterizado como pesquisa descritiva e utiliza a estratégia de estudo de caso de abordagem qualitativa para avaliar a SI com base em alguns controles da ABNT ISO/IEC 27001/2013 no departamento de recursos humanos.

Do ponto de vista de Lira (2019) a pesquisa descritiva possui objetivo de avaliar as características de determinado grupo, e por sua vez o estudo de caso aprofundam essas análises, como reforça Yin (2015), o estudo de caso permite restringir a pesquisa a um caso e dele almeja compreensão holística.

A empresa estudada é de pequeno porte, está localizada em no município de Piracicaba interior do Estado de São Paulo, e se enquadra no ramo de atividade de tecnologia da informação.

Com relação à pesquisa de campo é aplicado um questionário com perguntas abertas e fechadas no departamento de recursos humanos com intuito de levantar as informações dos controles selecionados como demonstra a figura 3.

Figura 3 - Controles selecionados

A.5	**Seção 5 - Políticas da segurança da informação**
A.5.1	Orientação da direção para segurança da informação
A.6	**Seção 6 - Organização da segurança da informação**
A.6.2	Dispositivos móveis e trabalho remoto
A.6.2.1	Política para o uso de dispositivo móvel
A.6.2.2	Trabalho remoto
A.7	**Seção 7 - Segurança em recursos humanos**
A.7.1	Antes da contratação
A.7.1.1	Seleção
A.7.1.2	Termos e condições de contratação
A.7.2	Durante a contratação
A.7.2.1	Responsabilidades da direção
A.7.2.2	Conscientização, educação e treinamento em segurança da informação
A.7.2.3	Processo disciplinar
A.7.3	Encerramento e mudança da contratação
A.7.3.1	Responsabilidades pelo encerramento ou mudança da contratação
A.9	**Seção 9 - Controle de acesso**
A.9.1	Requisitos do negócio para controle de acesso
A.9.1.1	Política de controle de acesso
A.9.1.2	Acesso as redes e aos serviços de rede
A.9.2	Gerenciamento de acesso do usuário
A.9.2.1	Registro e cancelamento de usuário
A.18	**Seção 14 - Conformidade**
A.18.1	Conformidade com requisitos legais e contratuais
A.18.1.4	Proteção e privacidade de informações de identificação de pessoal

Fonte: elaborado pelos autores, 2023

Ainda na visão de Lira (2019) o questionário é um bom instrumento de pesquisa quando há o intuito de permitir ao respondente justificar, bem como expressar opinião se concorda ou não com determinada indagação.

Por fim a utilização da NBR ISO/IEC 27001:2013 tem propósito de alicerçar o conjunto de questões, uma vez que é um *framework* de mercado, e, portanto, verificar com os resultados a possibilidade de avaliar qual o grau de maturidade dos controles adotados pela empresa, e o quanto são aderentes aos trabalhos realizados no dia a dia.

3.1. Avaliação do nível de maturidade

Os níveis de maturidade do COBIT foram selecionados como ferramenta para mensurar e comparar a proposta dos controles da Norma ISO com o que é evidenciado e praticado pela empresa, e segundo Antonio (2020) o COBIT é um *framework* de governança e gestão de Tecnologia da Informação (TI) que estabelece cinco níveis de maturidade para avaliação de seus processos.

Os níveis de maturidade do COBIT indicam o nível de eficiência, eficácia e

confiabilidade dos processos de TI em uma escala do nível 0 a 5, que são conforme Isaca (2018) nível 0 (processo incompleto) quando não há evidencia sistêmica de que o processo atinge seu objetivo, nível 1 (processo executado) quando o processo é executado, mas não há padrão, nível 2 (processo gerenciado) quando o processo é executado de forma administrativa (planejada, monitorado e ajustado) e o produto do trabalho são adequadamente estabelecidos e controlados, nível 3 (processo estabelecido) quando o processo é executado através de documentação padronizada, e são realizados treinamentos, nível 4 (processo previsível) é executado dentro de limites definidos e seus resultados são mensurados, e por fim nível 5 (processo otimizado) é o processo que esta em melhoria continua.

Em suma esta seção apresentou os cinco níveis de maturidade que o COBIT dispõe para avaliação dos controles praticados na empresa, e deste modo, permitir a comparação com o mercado, uma vez que o *framework* é amplamente reconhecido e utilizado. Portanto, cabe ressaltar que a empresa que adota a norma ISO 27001 pode se beneficiar do uso das métricas de avaliação de requisitos definidas pelo COBIT para avaliar os controles, e deste modo, alicerçar o SGSI implementado.

4. Resultados e Discussões

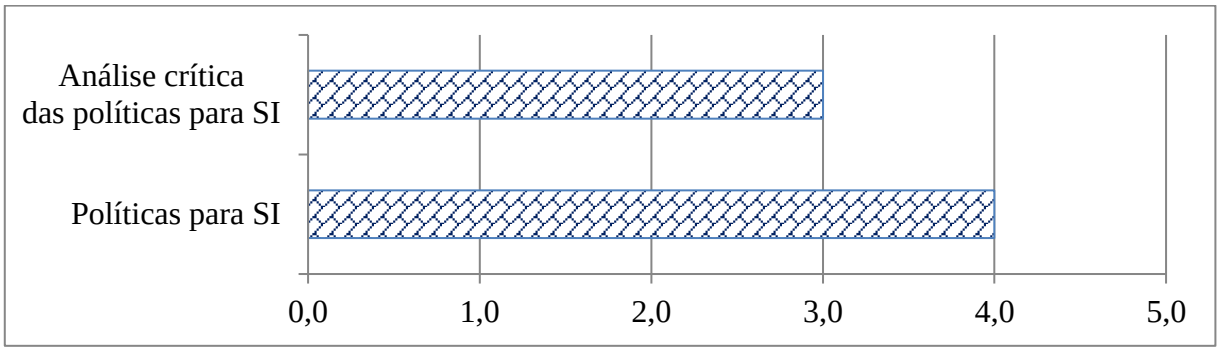
Neste capítulo são apresentados e discutidos os resultados da pesquisa de campo realizada através de questionário no departamento de RH. Os gráficos elaborados possuem a escala de 0 a 5 para demonstrar o nível de maturidade dos controles avaliados conforme estabelecido pelo COBIT.

No Gráfico 1 são apresentados os resultados da avaliação dos dois controles estudados, e como exibido no item “Políticas para SI”, a empresa possui avaliação 4 que significa que foi elaborada uma política de SI, e que também foi comunicado aos funcionários e partes externas relevantes. Em continuação ao trabalho, a empresa coletou assinatura dos funcionários para evidenciar a ciência dos profissionais.

O resultado do item “Políticas para SI” não pode ser avaliado como 5 devido à falta de continuidade de atualização da política de SI, e deste modo, o item “Análise crítica das políticas para SI” evidencia esse resultado, pois a empresa necessita adotar um cronograma de revisão das políticas para manter atualizado o seu SGSI. Sendo assim, com a média dos dois resultados o controle macro “Seção 5 - Políticas da segurança da

informação” tem avaliação de 3,5 (três e meio).

Gráfico 1 – Resultado dos controles avaliados da seção 5



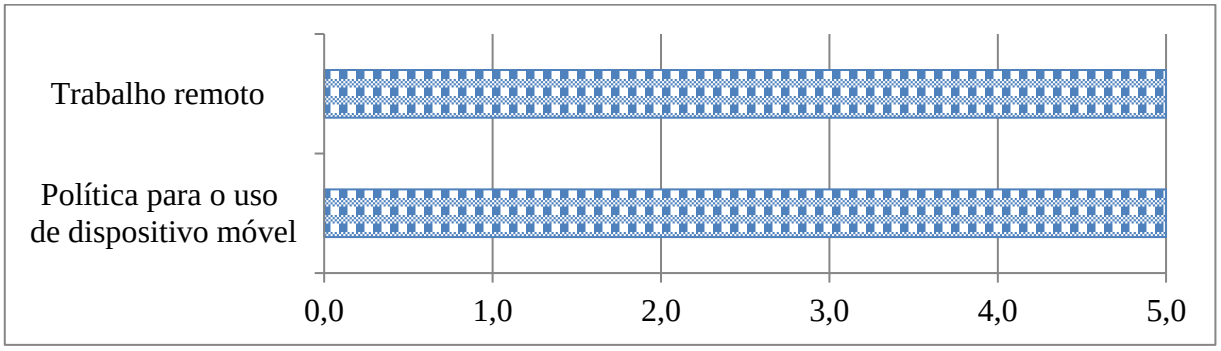
Fonte: elaborado pelos autores, 2023

No Gráfico 2 são apresentados os dois controles estudados da “Seção 6 - Organização da segurança da informação”, e como exibido os dois controles possuem nota 5, pois no item “Política para o uso de dispositivo móvel” a empresa elaborou a política requerida pelo controle, e também adotou um registro que evidencia o procedimento necessário para a utilização de dispositivo móvel com orientação do funcionário e recolhimento de assinatura.

No item seguinte, “Trabalho remoto”, a empresa também adotou uma política, e procedimento que evidencia a orientação e permissão que o funcionário possui para realização de trabalho remoto. Não somente, a empresa possui diversos mecanismos de segurança para realização deste tipo de trabalho, como exemplo acesso através da Virtual Private Network (VPN), notebook e celular corporativo, controle de acessos definidos, verificação de postura de segurança do dispositivo que realizará o acesso através de solução de segurança de Network Access Control (NAC), atualização dos equipamentos e ferramenta de trabalho colaborativo através do Microsoft 365.

Por fim, com a média dos dois resultados o controle macro da “Seção 6 - Organização da segurança da informação” tem como resultado a avaliação de 5 (cinco).

Gráfico 2 – Resultado dos controles avaliados da seção 6



Fonte: elaborado pelos autores, 2023

O Gráfico 3 exibe os controles relacionados ao departamento de recursos humanos, e são avaliados conforme os controles “Seleção”, com nota 5, pois a empresa adota no processo de seleção a verificação necessária do histórico do candidato conforme a lei, ética e regulamentações vigentes. Não obstante, faz uso de *checklist*, uma ferramenta, para auxiliar se o que é pedido ao candidato foi entregue por ele.

No item seguinte “Termos e condições de contratação”, a empresa deixa evidente no contrato de trabalho, no termo de confidencialidade e na autorização de uso de dados pessoais as responsabilidades de ambas as partes. Inclusive, adota nos contratos com terceiros o mesmo padrão conforme a necessidade. Ressalta-se que os contratos utilizados como modelo e os que são assinados com terceiros são revisados pelo departamento jurídico. Portanto, esse controle foi avaliado com nota 5 (cinco).

No item “Responsabilidade da direção”, a empresa deixa claro através dos documentos admissionais relacionados a SI e no curso de integração a responsabilidade do funcionário e de partes externas em relação à SI. Cabe ressaltar que os documentos envolvidos no curso de integração são assinados pelos funcionários e partes externas, e também há o reforço da necessidade de seguir estes regulamentos através do *e-mail*. Sendo assim, este item foi avaliado com nota 4 (quatro), devido a quantidade e qualidade dos elementos apresentados. Contudo é necessário ressaltar a importância de em intervalos regulares gerar novas evidências dos materiais para manter atualizado o SGSI da empresa.

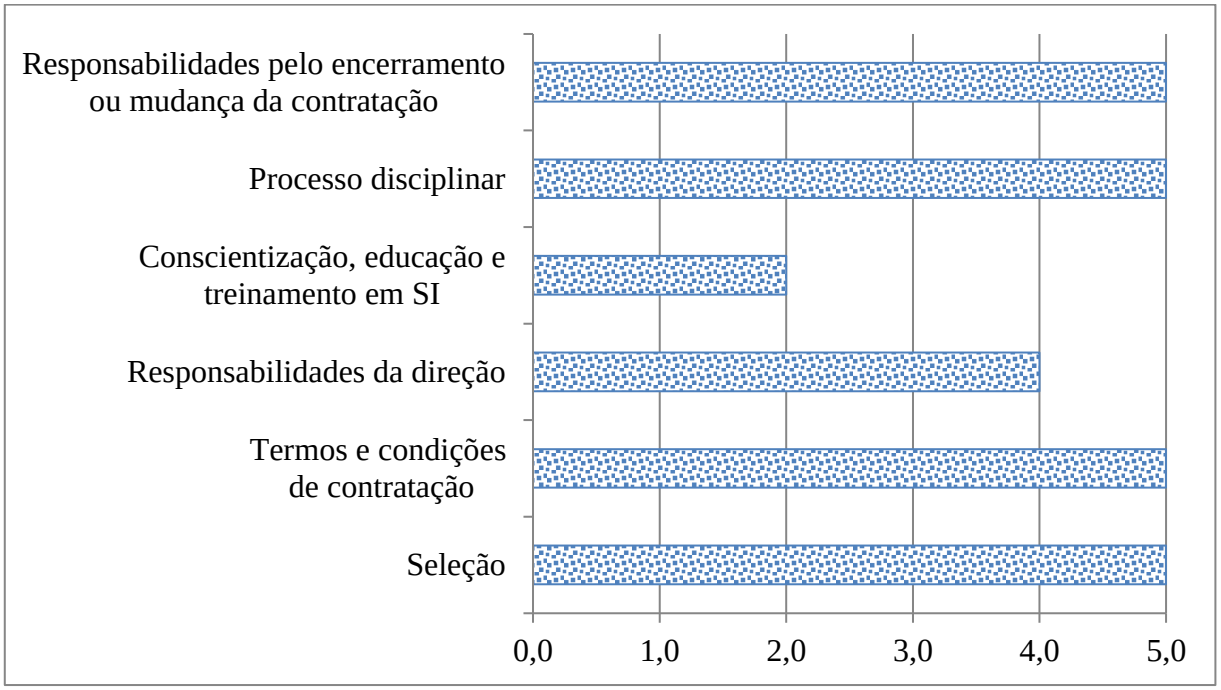
No item “Conscientização, educação e treinamento em SI”, pode-se avaliar que a empresa adota uma boa comunicação em relação a SI no processo de integração do

funcionário, no entanto, não mantém em intervalos regulares a conscientização formal, ou seja, com comunicados ou treinamentos. Embora realize quando necessário, através de *e-mail*, um informativo. Deste modo, esse controle foi avaliado com nota 2 (dois), pois o objetivo do controle é atingido de modo básico, porém completo, o que o caracteriza como realizado conforme nível de maturidade proposto pelo COBIT.

No próximo item "Processo disciplinar" a empresa evidencia o processo disciplinar formal que atende o item avaliado, tanto no contrato de trabalho, quanto na documentação de integração há menção desse controle. Em tempo, a empresa coleta assinatura dos funcionários como evidência de ciência da orientação fornecida, portanto, a nota avaliada é 5 (cinco).

No último item avaliado no departamento de RH, o item "Responsabilidade pelo encerramento ou mudança da contratação", a empresa trabalha esse controle no contrato de trabalho com a cláusula de confidencialidade, e também comunica sobre a necessidade de devolver os equipamentos, e abre chamado para a revogação dos acessos do funcionário.

Gráfico 3 – Resultado dos controles avaliados da seção 7



Fonte: elaborado pelos autores, 2023

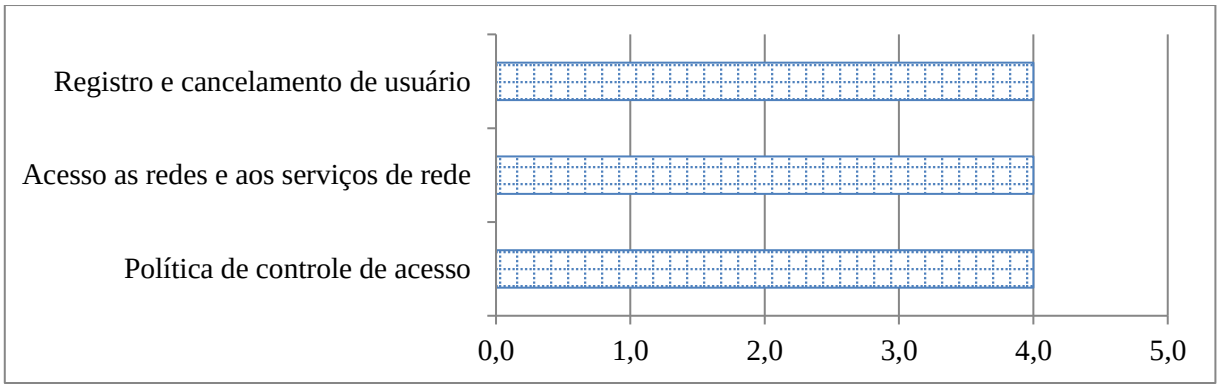
Nas situações que envolvem terceiros, há cláusula de confidencialidade nos documentos de contrato que, quando são assinados, envolve a revisão do departamento jurídico. Portanto, a avaliação desse controle é nota 5 (cinco).

Para finalizar, a média dos resultados apresentados determina para o controle macro da "Seção 7 - Segurança em recursos humanos" a avaliação de 4,56 (quatro inteiros e cinquenta e seis centésimos).

O Gráfico 4 apresenta três controles estudados da "Seção 9 - Controle de acesso", e como exibido os três itens são avaliados com nota 4 (quatro), pois em "Política e controle de acesso", a empresa possui implantado este controle, no entanto, não realiza a revisão em intervalos regulares, e através da política é estabelecido o procedimento em que o RH solicita o primeiro acesso do funcionário com acesso mínimo de liberação necessário para que as áreas da empresa tenha informações para estender o nível de acesso de acordo com a função executada.

No controle seguinte "Registro e cancelamento de usuário", a empresa tem um processo formal de registro e cancelamento de acessos que funciona através do sistema de chamado ou através de *e-mail*. Por fim, com a média dos resultados o controle macro da seção é nota 4 (quatro).

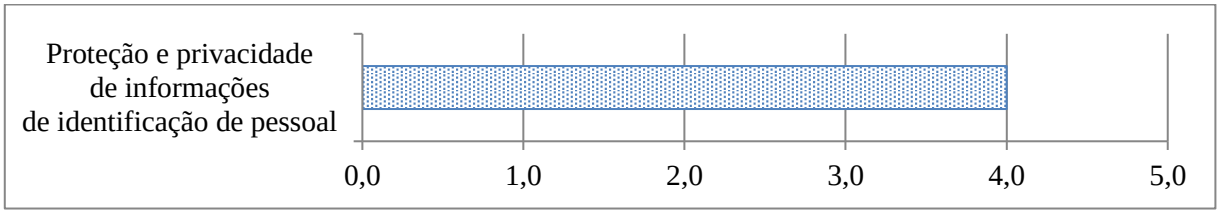
Gráfico 4 – Resultado dos controles avaliados da seção 9



Fonte: elaborado pelos autores, 2023

O Gráfico 5 apresenta o controle estudado referente a "Seção 14 - Conformidade", e exibe no item "Proteção e privacidade de informações" a nota 4 (quatro), portanto a nota geral da seção também é 4 (quatro), pois a empresa adotou a padronização de processos que atendem esse controle em função da Lei Geral de Proteção de Dados (LGPD).

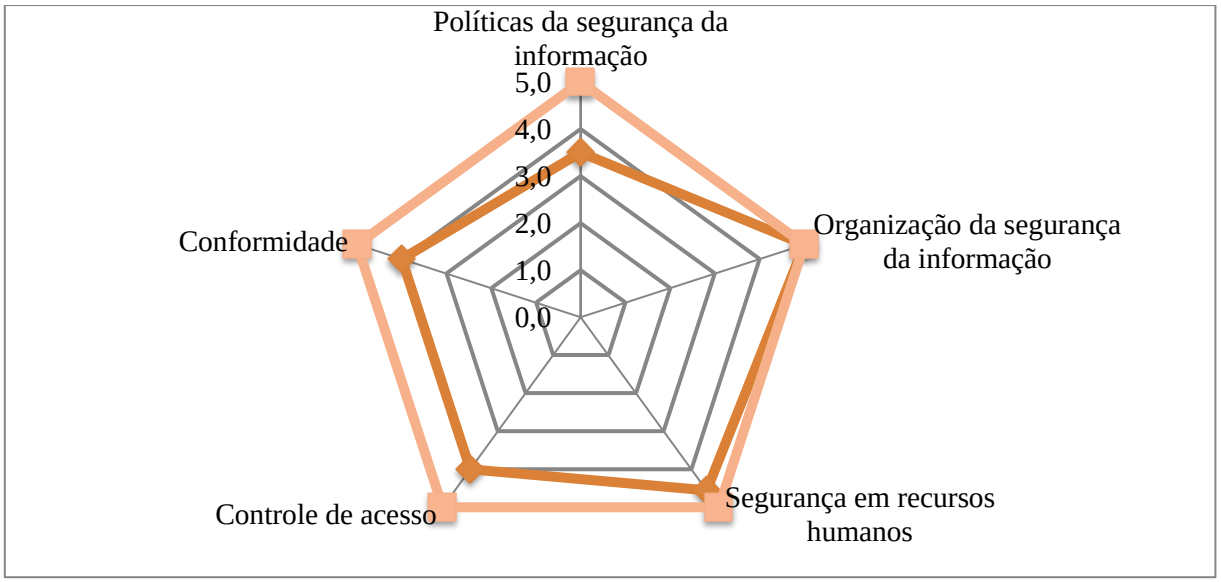
Gráfico 5 – Resultado do controle avaliado da seção 14



Fonte: elaborado pelos autores, 2023

Para finalizar no Gráfico 6, são apresentados os resultados dos controles das seções avaliadas que são as médias dos resultados obtidos nos controles de cada seção a saber seção 5: políticas de segurança da informação, seção 6: organização da segurança da informação, seção 7: segurança em recursos humanos, seção 9: controle de acesso, e seção 14: conformidade.

Gráfico 6 – Resultado da avaliação do nível de maturidade dos controles macros



Fonte: elaborado pelos autores, 2023

Nesta seção foram apresentados e discutidos os resultados da pesquisa de campo, e se pode observar que a empresa estudada exibiu bons resultados na avaliação, pois apresentou conformidade com os controles estudados e boas evidencias para sustentar seu SGSI.

Embora seja uma empresa recente no município, devido sua característica de prestadora de serviço para grandes empresas, foi observado que os controles avaliados foram trabalhados anteriormente no processo de adequação dos procedimentos internos

para atendimento a Lei Geral de Proteção de Dados Pessoais (LGPD).

Diante disso, a NBR ISO/IEC 27001/2013, como *framework* de mercado que trata do SGSI, demonstra sua importância, pois atende não somente a exigência de uma legislação recente, como também diversos processos necessários para a proteção da informação.

Para encerrar esta seção, se pode observar a utilização da NBR ISO/IEC 27001/2013 com as métricas de nível de maturidade do COBIT, e como ambos se mostraram excelentes ferramentas para avaliação dos controles estudados.

5. Considerações Finais

O tema SI é vasto, portanto, muitos caminhos podem ser explorados, e, certamente, como visto na revisão de literatura diferentes pessoas enxergam a SI de modos distintos, até mesmo dentro de uma mesma empresa. Sendo assim, respaldado pela compreensão da SI fornecida pela ABNT este trabalho explorou esta dinâmica dentro do departamento de RH de uma empresa de tecnologia.

Para alcançar os objetivos que são *i.* avaliar o departamento de RH de uma empresa de tecnologia da cidade de Piracicaba\SP em relação a SI com base em alguns controles da norma NBR ISO/IEC 27001/2013, e *ii.* realizar uma pesquisa bibliográfica sobre a SI aplicada ao Departamento de RH foi realizada uma pesquisa de campo com intuito de evidenciar os conceitos explorados na revisão de literatura.

Ambos os objetivos propostos são concluídos neste trabalho, de modo que a princípio a revisão de literatura tem o intuito de acompanhar a evolução do departamento de RH que foi se estruturando a partir da Revolução Industrial, e compreender como um *framework* de mercado aborda a SI neste departamento para que fosse possível analisar através de estudo de caso uma empresa real.

Alicerçado pelos conceitos aprendidos e as análises efetuadas se verificou que a empresa estudada, mesmo não tendo realizado um trabalho de certificação em SI, devido sua natureza de prestadora de serviços para grandes empresas e o desenvolvimento de seus processos para adequação a LGPD, conseguiu alcançar um bom nível de maturidade nos controles que foram selecionados.

Não obstante aliar a norma NBR ISO/IEC 27001/2013 com as métricas de nível

de maturidade do COBIT cria uma poderosa ferramenta prática para avaliação dos controles propostos. E ainda, permite gerar evidências concretas que possibilita que este estudo de caso possa ser comparado com outros.

Embora o objetivo de comparação não seja objeto deste trabalho, as evidências são referência para a empresa criar um plano de ação e melhorar seus controles com vista a atingir um nível de processo otimizado.

Em suma ao utilizar alguns controles da norma NBR ISO/IEC 27001/2013 aliada às métricas de nível de maturidade do COBIT, se pode avaliar o departamento de RH de uma empresa de TI, e constatar que esta alcançou um bom nível de maturidade nos controles estudados através do desenvolvimento das políticas, procedimentos, treinamentos, e também utilização de um arcabouço de ferramentas técnicas como VPN, NAC, controle de acesso e disponibilização de equipamentos aos funcionários para criar e manter seu Sistema de Gestão de Segurança da Informação.

Referências

ABNT. Tecnologia da informação - técnicas de segurança - código de prática para controles de segurança da informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro, p. 99. 2013. (9788507046134).

ABNT. Tecnologia da informação - técnicas de segurança - sistemas de gestão da segurança da informação - requisitos. Associação Brasileira de Normas Técnicas. Rio de Janeiro, p. 30. 2013. (9788507046080).

ABNT. Técnicas de segurança - extensão da ABNT ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação - requisitos e diretrizes. Associação Brasileira de Normas Técnicas. Rio de Janeiro, p. 82. 2019. (9788507083559).

ABNT. Quem somos, 2022. Disponível em: <https://www.abnt.org.br/institucional/sobre>. Acesso em: 13 Outubro 2022.

ANTONIO, A. M. Os 5 modelos de maturidade pelas diretrizes do COBIT. PMG academy, 2020. Disponível em: <https://www.pmgacademy.com/blog/artigos/cobit-modelos-maturidade/>. Acesso em: 20 Março 2023.

BORELLI, A. et al. LGPD - Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters, 2019. 474 p. ISBN 9786550650230.

CALDER, A.; WATKINS, S. IT governance an international guide to data security and ISO27001/ISO27002. 7ª. ed. United States: Kogan Page, 2020. 408 p. ISBN

9781789660302.

ELIA, B. B. D. O profissional de recursos humanos. São Paulo: Senac, 2021. 232 p. ISBN 9786555366907.

FERREIRA, S. D. C. Sistemas de informação em segurança. Londrina: Editora e Distribuidora Educacional SA, 2017. 224 p. ISBN 9788552202257.

ISACA. Cobit 2019 Framework: governance and management objectives. Schaumburg: Isaca, 2018. ISBN 9781604207286.

ISO. Information technology - security techniques - information security management systems - overview and vocabulary. International Organization for Standardization. Geneva, p. 34. 2018. (ISO/IEC 27000:2018(E)).

LANDOLL, D. J. Information security policies, procedures, and standards. Florida: Auerbach Publications, 2016. 254 p. ISBN 9781482245899.

LIRA, B. C. O passo a passo do trabalho científico. Petrópolis: Vozes, 2019. 96 p. ISBN 9788532648198.

MELLO, D. Home office foi adotado por 46% das empresas durante a pandemia. Agência Brasil, 2020. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2020-07/home-office-foi-adotado-por-46-das-empresas-durante-pandemia>. Acesso em: 19 Março 2023.

RIBEIRO, A. D. L. Gestão de pessoas. 2ª. ed. São Paulo: Saraiva, 2017. 301 p. ISBN 9788502178892.

SCHREINER, E.; BUSANELLO, M. Assistente de recursos humanos: rotinas de trabalho, perfil profissional. 2ª. ed. São Paulo: Senac, 2018. 144 p. ISBN 9788539622184.

SMULDERS, A. et al. Fundamentos de segurança da informação com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018. 256 p. ISBN 9788574528601.

SUDOSKI, B. S. Um estudo de caso de desenvolvimento de políticas de segurança da informação, com base nas normas ABNT NBR ISO/IEC:27000, para uma instituição de soluções tecnológicas. Trabalho de conclusão de curso, Universidade Federal de Santa Catarina, Florianópolis, p. 114. 2017.

VOLCHKOV, A. Information security governance - framework and toolset for CISOs and decision makers. Geneva: Auerbach Publications, 2018. 274 p. ISBN 9780815356448.

YIN, R. K. Estudo de caso planejamento e métodos. 5. ed. Porto Alegre: Bookman, 2015. 320 p. ISBN 9788582602317.