FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

FRANCISCO AMÉRICO DA SILVA

AVALIAÇÃO DO DEPARTAMENTO DE RECURSOS HUMANOS DE UMA EMPRESA DE TECNOLOGIA DA CIDADE DE PIRACICABA/SP EM RELAÇÃO À SEGURANÇA DA INFORMAÇÃO COM BASE EM ALGUNS CONTROLES DA NBR ISO/IEC 27001/2013

Americana - SP
2023

FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Francisco Américo da Silva

Avaliação do departamento de recursos humanos de uma empresa de tecnologia da cidade de Piracicaba/SP em relação à segurança da informação com base em alguns controles da NBR ISO/IEC 27001/2013

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Me. Edson Roberto Gaseta.

Área de concentração: Segurança da Informação.

Americana - SP
2023

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi-CEETEPS Dados Internacionais de Catalogação-na-fonte

SILVA, Francisco Américo da

Avaliação do departamento de recursos humanos de uma empresa de tecnologia da cidade de Piracicaba/SP em relação à segurança da informação com base em alguns controles da NBR ISO/IEC 27001/2013. / Francisco Américo da Silva – Americana, 2023.

48f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Edson Roberto Gaseta

1. Auditoria em sistemas de informação. I. SILVA, Francisco Américo da II. GASETA, Edson Roberto III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681.518.3

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Francisco Américo da Silva

Avaliação da segurança da informação no departamento de recursos humanos de uma empresa de tecnologia da cidade de Piracicaba/SP com base na norma NBR ISO/IEC 27001/2013

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

Área de concentração: Segurança da Informação.

Americana, 15 de junho de 2023.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Mestre
Fatec Americana

Rodrigo Brito Battilana (Membro)
Mestre
Fatec Americana

Maxwel Vitorino da Silva (Membro)
Mestre
Fatec Americana

AGRADECIMENTOS

Ao professor **Edson Roberto Gaseta** pelas orientações e acompanhamento do desenvolvimento deste trabalho.

Aos **professores membros da banca de aprovação** que compartilharam um pouco de seus conhecimentos para tornar este trabalho ainda melhor.

Aos **professores e funcionários da Fatec de Americana** que fazem um trabalho excepcional para que a instituição continue sendo bem reconhecida pela excelente formação de seus alunos.

A **empresa** que cedeu o espaço para realização dessa pesquisa e compartilhou um pouco de seus processos e conhecimentos.

E aos **amigos e familiares** que me acompanharam e certamente continuarão me acompanhando em meus projetos.

“Security is not a product, but a process. It's more than designing strong cryptography into a system; it’s designing the entire system such that all security measures, including cryptography, work together”

Bruce Schneier

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.

LISTA DE GRÁFICOS

SUMÁRIO

1. INTRODUÇÃO

A temática Segurança da Informação (SI) tem se tornado rotineira na vida das pessoas e das organizações, seja em relação a segurança de seus equipamentos pessoais ou na proteção dos ativos das empresas, ou ainda na leitura de reportagens sobre algum vazamento de dados e até mesmo em relação às novas regulamentações aprovadas como a Lei Geral de Proteção de Dados (LGPD).

Nesse contexto o presente estudo explora a temática da SI direcionada ao Departamento de Recursos Humanos (RH), uma tarefa que envolve tanto empresas como pessoas.

A princípio a revisão bibliográfica busca esclarecer o conceito de Segurança da Informação (SI), e explicar 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”.

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

Para findar a proposta desse projeto o conteúdo contempla diversas matérias do curso de Segurança da Informação como Políticas de Segurança da Informação, Auditoria em Sistemas de Informações e Análise e Gestão de Riscos em Segurança da Informação.

1.1 Objetivo Geral

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.

1.2 Objetivos Específicos

- Realizar uma pesquisa bibliográfica sobre a Segurança da Informação (SI) aplicada ao Departamento de Recursos Humanos (RH).

- Coletar dados por meio de questionário aplicado ao Departamento de Recursos Humanos (RH).

2. REVISÃO BIBLIOGRÁFICA

A revisão de literatura apresentada tem o intuito de formar um panorama geral da segurança da informação, apresentar o departamento de recursos humanos e comentar sobre sua importância nas organizações, introduzir a ISO 27001 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 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 segurança da informação às situações que estão próximas às suas atividades diárias. Portanto, não visualizam com plenitude a real importância do tema.

Para um especialista a segurança da informação 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 o significado de segurança da informação 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 segurança da informação 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 segurança da informação 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 segurança da informação 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, no mínimo, 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, sem dúvida, 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, principalmente, de tecido (SCHREINER e BUSANELLO, 2018).

No período as primeiras fábricas criaram um cenário que permitia a entrega de grandes quantidades de produtos, diferentemente do trabalho artesanal, e isso gerou a necessidade de mais pessoas trabalhando. Consequentemente surge o Departamento Pessoal (DP), que na realidade era o próprio dono, e tinha a

incumbência básica 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 havia 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 Departamento Pessoal (DP) também mudou, se tornou profissional.

Naturalmente, o DP nunca deixou de existir, na realidade, com o surgimento dos sindicatos e pressões da sociedade os trabalhadores conquistaram e passou a ser direito a admissão através de contrato de trabalho, período de férias e jornadas de trabalho normatizadas (ELIA, 2021).

Mais adiante o DP se torna uma parte do que é conhecido como departamento de RH ou também Gestão de Pessoas (GP) uma área que compreende diversos subsistemas como recrutamento e seleção, treinamento e desenvolvimento, avaliação de desempenho, cargos e salários, folha de pagamento, benefícios, relações sindicais, e segurança e medicina do trabalho (RIBEIRO, 2017).

Por conseguinte evidência se que 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 nenhuma organização ou setor específico, 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).

Contudo, mesmo que a empresa não almeje uma certificação, na visão de Landoll (2016) há bons motivos para seguir suas diretrizes, pois além do seu reconhecimento, também é possível utilizá-la como guia, e devido a sua ampla adoção no mercado há diversas referências que a mapeiam em conjunto com outros *frameworks* como COBIT e NIST.

Dos 14 grupos que são referenciados no Anexo A da NBR ISO/IEC 27001/2013, e que estão representados no Quadro 1, o grupo A.7 Segurança em recursos humanos é de fundamental importância para este estudo.

Quadro 1 - Grupos de controle ISO/IEC 27001/2013

ORDEM	GRUPOS DE CONTROLE	
1	A.5	Políticas de segurança da informação
2	A.6	Organização da segurança da informação
3	A.7	Segurança em recursos humanos
4	A.8	Gestão de ativos
5	A.9	Controle de acesso
6	A.10	Criptografia
7	A.11	Segurança física e do ambiente
8	A.12	Segurança nas operações
9	A.13	Segurança nas comunicações
10	A.14	Aquisição, desenvolvimento e manutenção de sistemas
11	A.15	Relacionamento na cadeia de suprimento
12	A.16	Gestão de incidentes de segurança da informação
13	A.17	Aspectos da segurança da informação na gestão da continuidade do negócio
14	A.18	Conformidade

Fonte: adaptado ABNT, 2013

Diante do Quadro 1 apresentado se pode observar que a NBR ISO/IEC 27001/2013 abrange a segurança em todos os aspectos da organização, portanto para direcionar os estudos a seção seguinte tem o intuito de aprofundar os controles de segurança para recursos humanos.

2.4 Segurança em recursos humanos

Conforme apresentação do Quadro 2, a segurança em recursos humanos é abordada sob três perspectivas, sendo: *i.* antes da contratação, *ii.* durante a contratação e *iii.* encerramento e mudança da contratação.

Quadro 2 - Grupos de controle de segurança em RH da ISO/IEC 27001/2013

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

Entretanto cabe ressaltar que embora a norma certificadora para as empresas seja a NBR ISO/IEC 27001/2013, insere-se no contexto a NBR/IEC 27002/2013 denominada “Tecnologia da informação - técnicas de segurança - código de prática para controles de segurança da informação” que de acordo com a ABNT (2013) é um guia de referência para implantação e manutenção de um sistema de gestão de segurança da informação.

Ainda em relação às normas e com a preocupação da privacidade de dados pessoais foi elaborada a NBR ISO/IEC 27701/2019 com nome “Técnicas de segurança - extensão da ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação - requisitos e diretrizes”.

Em síntese, até o momento se pode verificar ao menos três normas que estão relacionadas à segurança da informação no processo de recursos humanos, a ISO 27001, 27002 e a 27701.

Com o conhecimento das normas que são abordadas 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 ISO 27002 deixa evidente que todos os funcionários são responsáveis pela segurança da informação, e ainda se pode ressaltar que é de suma importância o desenvolvimento de procedimentos rigorosos 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 à segurança da informação, deste modo é claro que se trata de um processo pré-triagem para contratação, e no qual enseja verificar informações de cunho pessoal e profissional como a exatidão do currículo, informações acadêmicas e profissionais, verificação de identidade incluindo visto de trabalho, verificação de crédito 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 cargos 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 segurança da informação, 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. Ressaltam o encerramento, pois os funcionários durante a vigência do contrato têm acesso a diversas informações, e devem mantê-las confidenciais mesmo após o vínculo empregatício ter se encerrado.

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 com clareza que promover seu 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, e atribui a direção essa incumbência.

Nesse contexto conforme Smulders *et al.* (2018) é necessário trabalhar no treinamento de integração o tema segurança da informação, 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.

A NBR ISO/IEC 27701:2019 traz um adendo em relação aos treinamentos, e observa a necessidade da periodicidade, mas também a seleção de conteúdos, de tal modo que funcionários com acesso a dados pessoais, por exemplo, devem ser treinados apropriadamente para lidar com esse tipo de informação.

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 ao funcionário para que possa realizar o treinamento em momentos de disponibilidade, além de incluir testes, jogos e materiais diversos como áudio e vídeo.

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, e recomendam que sejam comunicados, também, nos contratos de trabalhos, em adição 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 atendimento desse 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, acrescenta Calder e Watkins (2020) no processo de entrevista de desligamento.

Em resumo são diversos os aspectos relacionados à segurança da informação 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 também visualizar que muitos dos itens mencionados trazem uma bagagem de outras seções. Dessa forma, é de fundamental importância manter uma visão holística da gestão de recursos humanos para que sejam assegurados os princípios da segurança da informação (confidencialidade, integridade e disponibilidade) em cada um dos seus processos.

2.5 Controles relacionados

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 recursos humanos.

Quadro 3 - Controle de segurança adicionais para RH extraídos de outras seções da ISO/IEC 27001/2013

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). Contudo, não é simples desenvolver uma

visão clara do cenário ou do que pode ser realizado, por este motivo desenvolver uma Política de SI é um processo interativo e que requer o envolvimento de todos os departamentos (VOLCHKOV, 2018).

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 a partir do surto de 2019, quando o governo declarou diversas medidas, entre elas a quarentena, para enfrentar o estado de emergência de saúde pública de importância internacional decorrente do coronavírus.

Na época:

> O trabalho em casa foi estratégia adotada por 46% das empresas durante a pandemia, segundo a Pesquisa Gestão de Pessoas na Crise covid-19. O estudo elaborado pela Fundação Instituto de Administração (FIA) coletou, em abril, dados de 139 pequenas, médias e grandes empresas que atuam em todo o Brasil. O percentual de companhias que adotou o teletrabalho durante a quarentena foi maior no ramo de serviços hospitalares (53%) e na indústria (47%). Entre as grandes empresas, o índice das que colocaram os funcionários em regime de home office ficou em 55% e em 31%, entre as pequenas. Um terço do total das empresas (33%) disse que adotou um sistema parcial de trabalho em casa, valendo apenas em alguns dias da semana (MELLO, 2020, on-line).

Com este contexto, é impreterível para empresa adotar uma política de trabalho remoto, uma vez que as medidas de proteção disponíveis dentro da organização possivelmente 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 e também que a empresa deve adotar controles para o gerenciamento de acesso do usuário (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 que são relevantes para o desenvolvimento dos trabalhos no departamento de RH, pois a luz da política de segurança da informação é identificada a responsabilidade de cada departamento e funcionário, e a partir deste importante documento, a empresa adota os mecanismos de proteção necessários para o desenvolvimento de sua atividade.

2.6 Controles e níveis estratégicos

Esta seção apresenta os controles políticas, procedimentos e instruções de trabalho que são meios que a organização dispõe para modificar os riscos á segurança da informação.

Conforme afirma Andrade (2019) as empresas podem ser classificadas em relação aos níveis *i.* estratégico, *ii.* tático e *iii.* operacional de modo que cada nível desenvolve planejamentos para atingir os objetivos organizacionais.

Os planejamentos desencadeiam ações que envolvem os cargos da empresa de modo diferenciado (BRAQUEHAIS, 2020), isto, pois, os gestores precisam entender a organização como um todo, mas não poderiam a partir de um único nível dar conta de todos os processos. Portanto, a ramificação em níveis permite que o nível abaixo, execute com mais detalhes o que foi planejado no nível superior (SMULDERS *et al.*, 2018).

O nível estratégico é o mais alto em relação à hierarquia, composto pelo presidente e diretores executivos nas empresas de grande porte, já nas empresas de pequeno porte, o proprietário é a figura equivalente (ANDRADE, 2019).

No nível estratégico são desenvolvidas as políticas, ou seja, uma orientação formal escrita sobre o que a empresa espera em relação aos funcionários e a segurança da informação, por exemplo, (SMULDERS *et al.*, 2018).

No nível tático como aborda Andrade (2019), encontram-se os gestores dos níveis funcionais como gerente de *marketing*, gerente de recursos humanos e gerente de produção. Nesse ponto da hierarquia os dirigentes recebem o planejamento do nível acima, e precisam encontrar meios para implementação e coordenação.

É no nível tático que os procedimentos são elaborados, e neles são especificados como conduzir as atividades ou os processos (SMULDERS *et al.*, 2018).

O último nível é o operacional, e este tem intuito de manter as atividades do dia a dia em execução (SMULDERS *et al.*, 2018). Nesse nível se encontram as atividades operacionais como atendimento ao cliente, vendas e fechamento de frequência (ANDRADE, 2019).

O nível operacional desenvolve as instruções de trabalho que são de modo ilustrativo um passo a passo do que deve ser feito para alcançar os objetivos das políticas (SMULDERS *et al.*, 2018).

Compreender a estrutura da organização é de suma importância para que os controles possam ser utilizados adequadamente, pois há uma relação entre as políticas, procedimentos e instruções de trabalho, pois enquanto as políticas fornecem a base para estruturar o SGSI, os procedimentos e instruções de trabalho especificam em detalhes o quê, e como executar as atividades.

3. METODOLOGIA

O presente estudo é caracterizado como pesquisa descritiva que utiliza a estratégia de estudo de caso de abordagem qualitativa para avaliar a segurança da informação 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, anexo 1, é aplicado um questionário com perguntas abertas e fechadas no departamento de recursos humanos com intuito de levantar as informações dos controles selecionados do anexo A da NBR ISO/IEC 27001:2013, como demonstra o Quadro 4.

Quadro 4 - Grupos de controle ISO/IEC 27001/2013

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 pelo autor, 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.

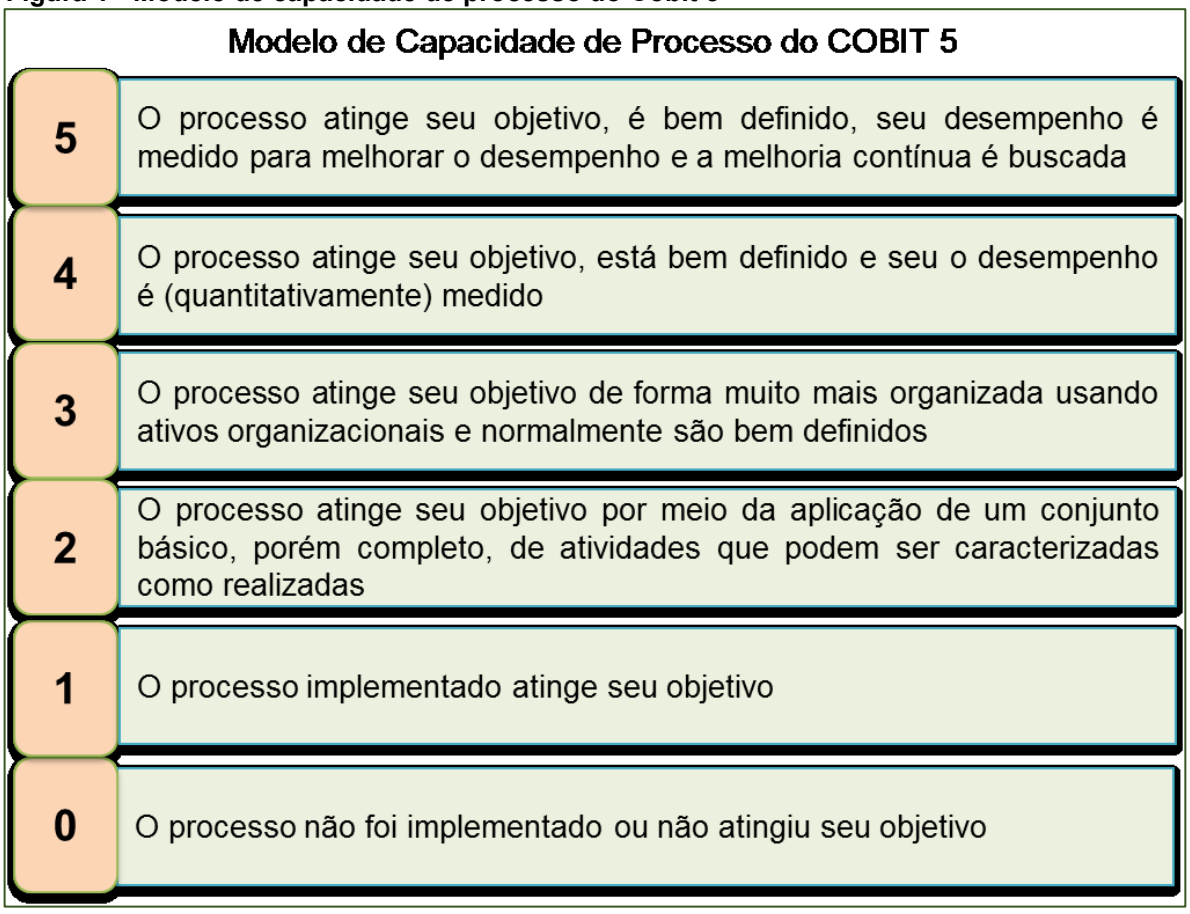
3.1 Avaliação do nível de maturidade

A norma ABNT ISO/IEC 27001/2013 estabelece os requisitos para compor o SGSI, e através da implementação dos controles a empresa se adequa ao cenário almejado. No entanto, a norma não informa como fazer a implantação, e tampouco como avaliar se o que foi implementado está adequado.

Na perspectiva de mensurar e permitir a comparação do que é realizado na empresa com o que é praticado na indústria, o COBIT, um *framework* de governança corporativa, estabelece um modelo de maturidade, ou seja, uma escala que de 0 a 5 para avaliação de seus requisitos (ANTONIO, 2020).

Conforme a Figura 1 é possível verificar que à medida que a empresa ganha maturidade em seus processos, a avaliação dos requisitos é melhorada, e este é o objetivo de se utilizar uma métrica para avaliação.

Figura 1 - Modelo de capacidade de processo do Cobit 5



Fonte: adaptado ISACA, 2018

A partir da ilustração se percebe que a Isaca (2018) determina:

- Nível 0 (processo incompleto): não há evidência sistêmica de que o processo atinge seu objetivo.
- Nível 1 (processo executado): processo executado, mas não há padrão.
- Nível 2 (processo gerenciado): processo executado de forma administrativa (planejada, monitorado e ajustado) e o produto do trabalho são adequadamente estabelecidos e controlados.
- Nível 3 (processo estabelecido): processo é executado através de documentação padronizada, e são realizados treinamentos.
- Nível 4 (processo previsível): processo é executado dentro de limites definidos e seus resultados são mensurados.
- Nível 5 (processo otimizado): processo é continuamente melhorado.

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

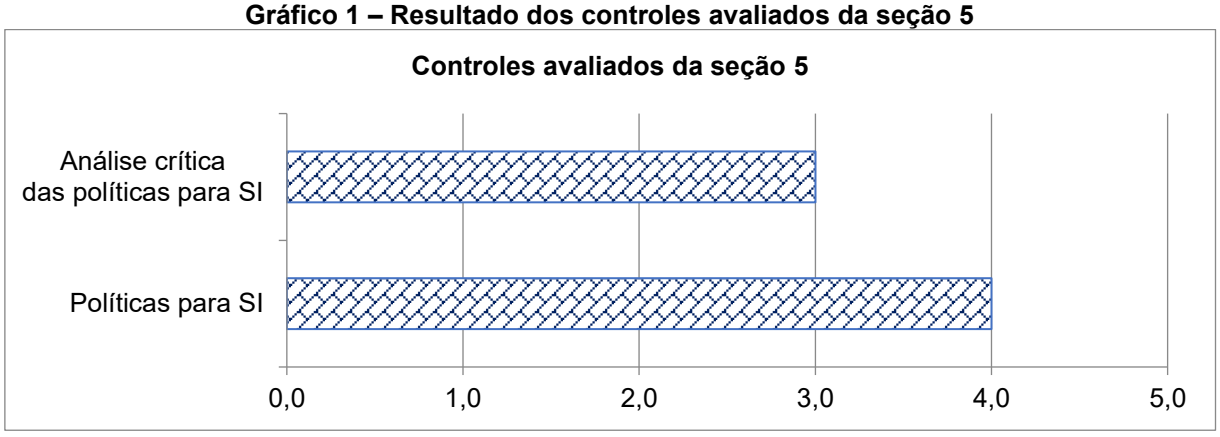
Neste capítulo são apresentados e discutidos os resultados da pesquisa de campo realizada através de questionário no departamento de recursos humanos da empresa estudada. Os gráficos elaborados possuem a escala de 0 a 5 para demonstrar o nível de maturidade dos controles avaliados.

4.1 Resultados

No Gráfico 1 são apresentados os resultados da avaliação dos dois controles estudados, e como exibido no controle “Políticas para SI”, a empresa possui avaliação 4 que significa que foi elaborada uma política de segurança da informação, 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 segurança da informação, 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



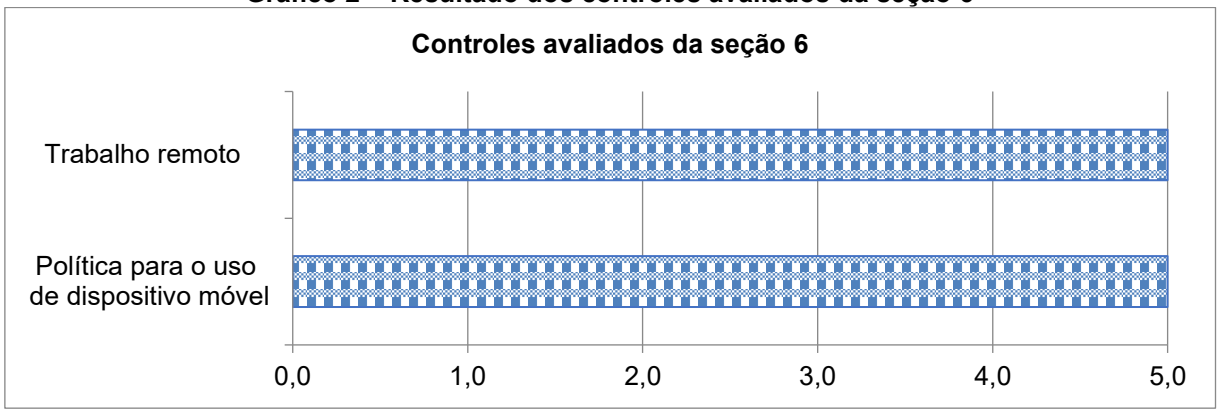
Fonte: elaborado pelo autor, 2023

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, 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 pelo autor, 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 segurança da informação. 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.

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

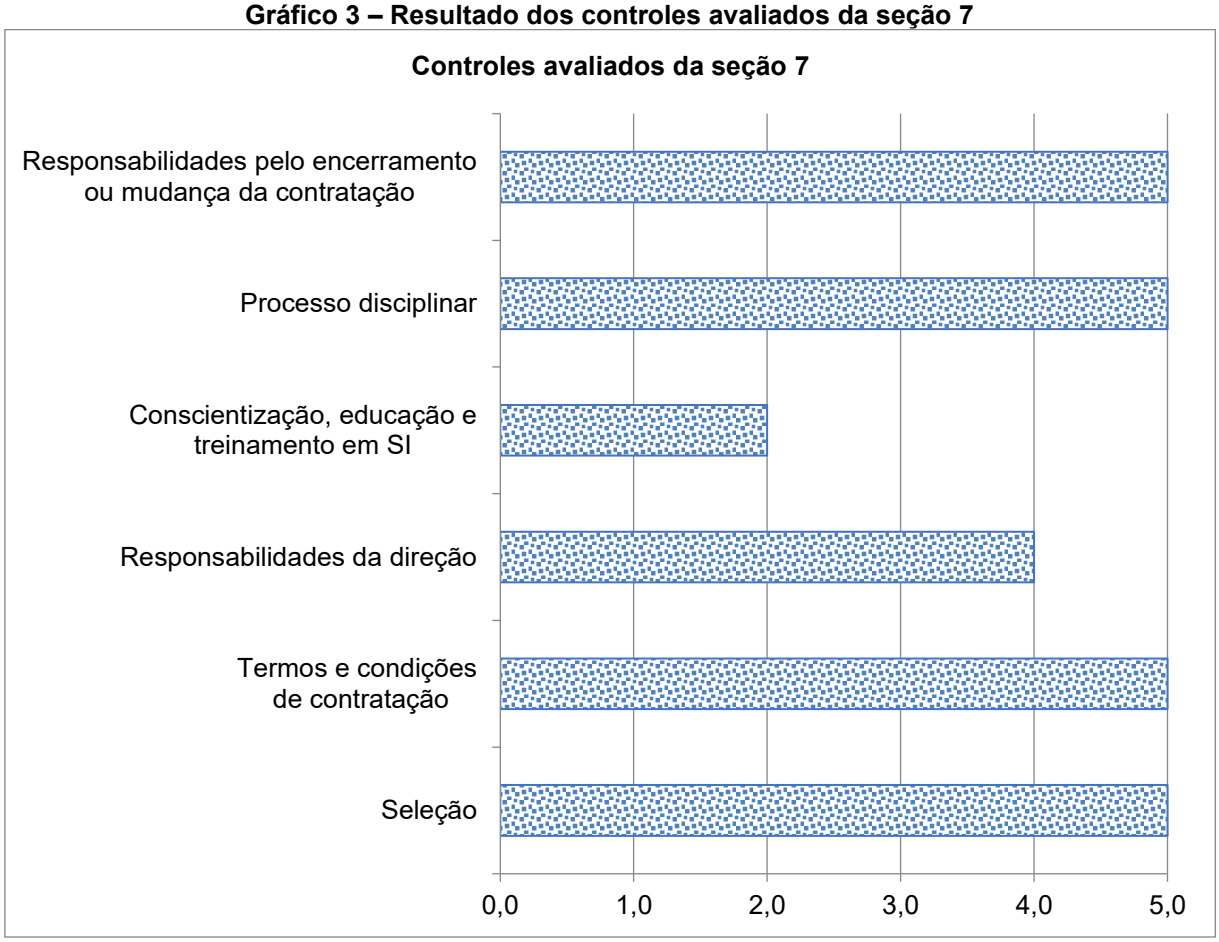
coleta assinatura dos funcionários como evidência de ciência da orientação fornecida, portanto, a nota avaliada é 5 (cinco).

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.

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).

Gráfico 3 – Resultado dos controles avaliados da seção 7

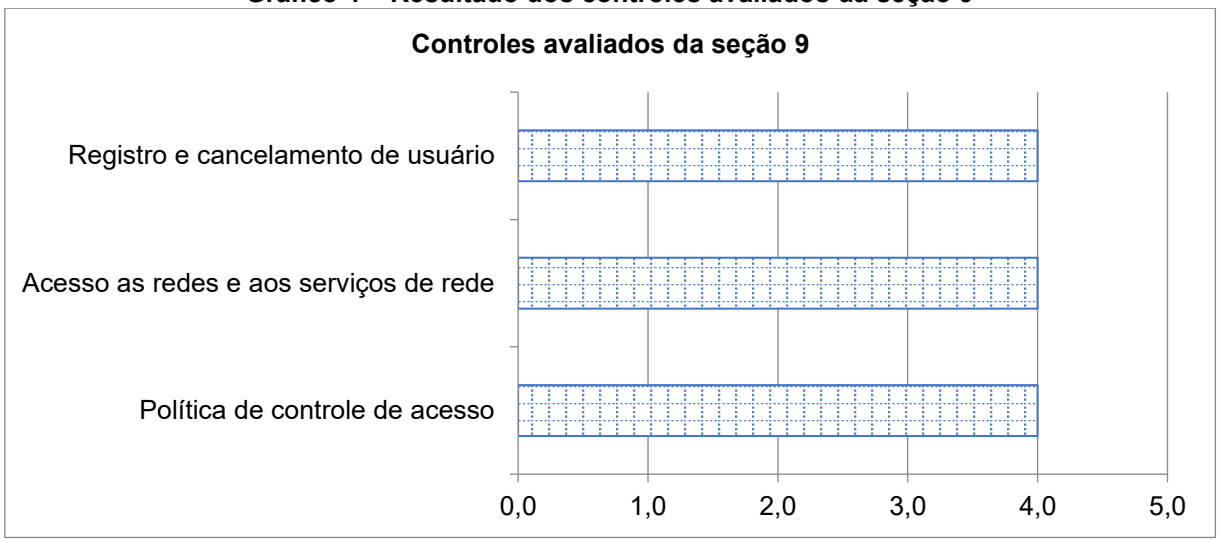


Fonte: elaborado pelo autor, 2023

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).

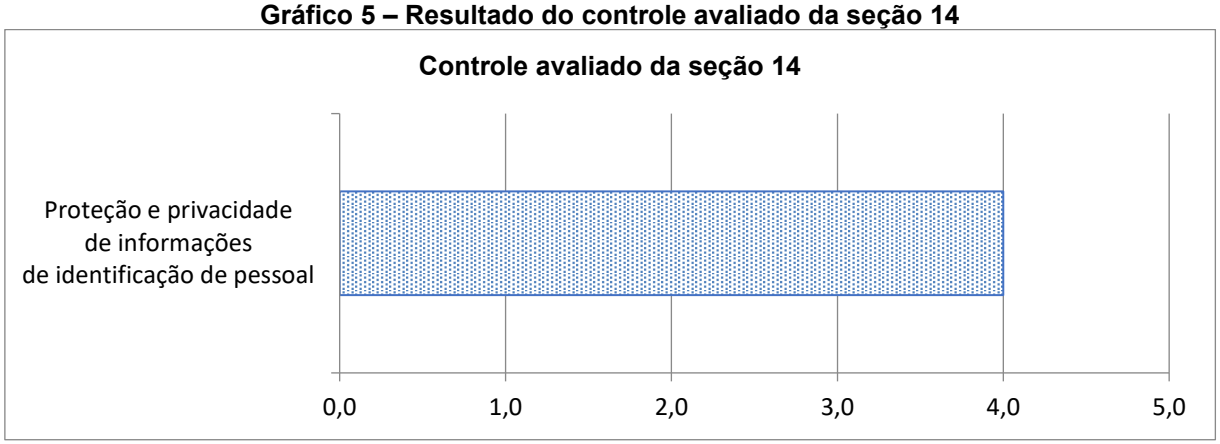
Gráfico 4 – Resultado dos controles avaliados da seção 9



Fonte: elaborado pelo autor, 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 pelo autor, 2023

Para finalizar no Gráfico 6, são apresentados os resultados dos controles macros avaliados.

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

Fonte: elaborado pelo autor, 2023

Nesta seção foram apresentados os resultados da pesquisa de campo realizada na empresa estudada, e estes resultados são discutidos na seção seguinte.

4.2 Discussões

Com panorama de avaliar o departamento de recursos humanos de uma empresa de tecnologia da cidade de Piracicaba/SP em relação à segurança da informação com base em alguns controles da NBR ISO/IEC 27001/2013 e realização da revisão de literatura e pesquisa de campo, pode-se avaliar o nível de maturidade da empresa em relação aos controles estudados.

A empresa estudada exibiu bons resultados na pesquisa de campo, e também apresentou as evidências necessárias para realização da avaliação dos controles analisados.

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.

A empresa se beneficiou do processo conduzido anteriormente visto as boas avaliações, no entanto, deixou de lado um item de extrema importância para a manutenção do SGSI que é a revisão periódica das políticas e procedimentos adotados.

Como visto na revisão de literatura, os processos de RH mudam ao longo do tempo, e com isso o SGSI também muda, e é através das atualizações das políticas e procedimentos que a empresa se mantém em conformidade com essas mudanças.

Ainda como observado na pesquisa de campo à empresa atingiu um alto grau de organização da SI e da segurança em recursos humanos, o que a beneficia para que com poucos ajustes alcance um “processo otimizado”, que é o de nível 5, na escala de avaliação de maturidade do COBIT, ou seja, um processo que é continuamente melhorado.

Sendo esta empresa prestadora de serviço para outras grandes empresas, também se pode avaliar o quanto é rigoroso o controle de acesso estabelecido, e,

portanto, extremamente bem desenvolvido. A empresa demonstra seriedade e capacitação dos profissionais contratados tanto do ponto de vista organizacional, com políticas e procedimentos bem estabelecidos, quanto do ponto de vista técnico, com a utilização de *softwares* e equipamentos modernos. Essas medidas garantem um bom desempenho do seu Sistema de Gestão de Segurança da Informação (SGSI).

Nesse sentido desenvolver uma política de SI em RH é de extrema importância para assegurar que o candidato esteja habilitado para exercer a função na qual ele foi contratado. E a empresa demonstrou que possui bem implantados os processos de RH conforme a nota próxima ao nível otimizado do controle.

Em continuação a discussão da avaliação e para finalizar esta seção, a empresa possui uma política de SI bem desenvolvida, e detalhada que envolve todos os seus processos. Inclusive, possui um bom treinamento de integração para os funcionários no qual ele toma ciência da documentação.

No entanto, foi o item que apresentou menor nota em comparação com os demais, e requer uma análise especial, pois dentro desse controle macro, o item “Análise crítica das políticas para segurança da informação”, foi o que impactou negativamente o resultado, uma vez que é requerido que dentro dos processos que envolvem o SGSI, e neste caso a documentação, seja revisada de acordo com um cronograma estabelecido. Muito embora a empresa realize a atualização quando há mudanças significativas, a literatura ressalta essa necessidade.

Em sequência é de suma importância manter a documentação atualizada, tanto para garantir o comprometimento da alta direção que se renova em períodos de quatro anos, quanto para que os funcionários tenham a ciência da importância das políticas e procedimentos envolvidos, uma vez que poderão ser aplicados treinamentos com intuito de reintegração.

Para encerrar esta seção, pode-se 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 segurança da informação 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 empresa. Sendo assim, respaldado pela compreensão da SI fornecida pela ABNT este trabalho explorou a 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 Segurança da Informação (SI) aplicada ao Departamento de Recursos Humanos (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 para este estudo.

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 permitem que este estudo de caso possa ser comparado com outros.

Embora o objetivo de comparação não seja objeto deste trabalho, as evidências servem como 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, controle de acesso e disponibilização de equipamentos aos funcionários para criar e manter seu Sistema de Gestão de Segurança da Informação.

6. 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.

ANDRADE, A. R. D. **Planejamento estratégico para pequenas empresas**. Rio de Janeiro: Alta Books, 2019. 224 p. ISBN 9788550806112.

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.

BRAQUEHAIS, A. **Gestão estratégica e estratégias inovadoras o essencial para alunos de graduação**. Brasilia: Antonio Braquehais, 2020. 155 p. ISBN 9786500039528.

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.

7. ANEXOS

7.1 ANEXO 1: Questionário da avaliação da segurança da informação

A.5.1.1: Há um conjunto de políticas de segurança da informação? (SIM\NÃO)
- Como foi comunicado aos funcionários e parte externas? (aberta)

A.5.1.2: Há um cronograma de revisão das políticas de segurança da informação? (SIM\NÃO)
- Se não, como funciona a atualização? (aberta)

A.6.2.1: Há políticas e medidas que apoiam a segurança da informação para gerenciar os riscos decorrentes do uso de dispositivos móveis? (SIM\NÃO)
- Como funciona? (aberta)

A.6.2.2: Há política e medidas implantadas que apoiam a segurança da informação e protegem as informações acessadas, processadas ou armazenadas em locais de trabalho remoto? (SIM\NÃO)
- Quais são essas medidas? (aberta)

A.7.1.1: Há verificação do histórico dos candidatos a emprego, de acordo com a ética, regulamentações e leis relevantes proporcionais aos requisitos do negócio, riscos percebidos e a classificação das informações acessadas? (SIM\NÃO)
- Como é realizada? (aberta)

A.7.1.2: Há declaração das responsabilidades dos contratados e da organização em contratos? (SIM\NÃO)
- Como funciona? (aberta)

A.7.2.1: A direção solicita aos funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização? (SIM\NÃO)
- Como funciona? (aberta)

A.7.2.3: Há um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação? (SIM\NÃO)
- Como funciona? (aberta)

A.7.3.1: Como funciona a questão das responsabilidades e obrigações em relação à segurança da informação que continuam vigentes no encerramento ou mudança da contratação? (aberta)

A.9.1.1: Há politica de controle de acesso documentada, estabelecida e de acordo com os requisitos de segurança da informação e do negócio? (SIM\NÃO)
- Como funciona? (aberta)

A.9.1.2: Os funcionários recebem somente os acessos às redes e serviços de rede que tenham sido especificamente autorizados a utilizar? (SIM\NÃO)
- Como funciona? (aberta)

A.9.2.1: Há um processo forma de registro e cancelamento de usuário implementado para permitir a atribuição dos direitos de acesso? (SIM\NÃO)
- Como funciona? (aberta)

A.18.1.4: Há mecanismos para assegurar a proteção das informações pessoais conforme requerido por legislação e regulamentação pertinente quando aplicável? (SIM\NÃO)
- Como funciona? (aberta)

7.2 ANEXO 2: Resultado da avaliação da segurança da informação

Ref	Titulo do Controle	Descrição do Controle	Nota	Comentários
A.5	**Seção 5 - Políticas da segurança da informação**		**3,5**	
A.5.1	Orientação da direção para segurança da informação	Objetivo: 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.5.1.1	Políticas para segurança da informação	Um conjunto de políticas de segurança da informação deve ser definido, aprovado pela direção, publicado e comunicado para os funcionários e partes externas relevantes.	4,0	A empresa elaborou um conjunto de políticas que atendem a este controle, e também comunicou os funcionários e partes externas relevantes. A empresa comunica os novos funcionários sobre as políticas. A empresa mantém um histórico com assinatura dos funcionários como evidência. Recomendação: em intervalos regulares realizar treinamento sobre as políticas para atender ao nível 5 de maturidade.
A.5.1.2	Análise crítica das políticas para segurança da informação	As políticas de segurança da informação devem ser analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para segurar a sua continua pertinência, adequação e eficácia.	3,0	A empresa não tem implementado cronograma de revisão das políticas completamente, no entanto, realiza atualizações quando há alterações significativas, e comunica os funcionários por e-mail no grupo da empresa. Recomendação: revisar as políticas em intervalos regulares, e inclusive adotar um padrão para o controle no SGSI e coletar as assinaturas dos envolvidos na revisão.

Ref	Titulo do Controle	Descrição do Controle	Nota	Comentários
A.6	**Seção 6 - Organização da segurança da informação**		**5,0**	
A.6.2	Dispositivos móveis e trabalho remoto	Objetivo: garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis		
A.6.2.1	Política para o uso de dispositivo móvel	Uma política e medidas que apoiam a segurança da informação devem ser adotadas para gerenciar os riscos decorrentes do uso de dispositivos móveis.	5,0	A empresa elaborou um conjunto de políticas que satisfazem esse controle, coleta as assinaturas dos funcionários e mantém atualizado o registro quando há alterações.
A.6.2.2	Trabalho remoto	Uma política e medidas que apoiam a segurança da informação devem ser implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.	5,0	A empresa elaborou um conjunto de políticas que satisfazem esse controle, coleta as assinaturas dos funcionários e mantém atualizado o registro quando há alterações. A empresa adota diversas medidas de segurança para proteger as informações em situação de trabalho remoto como: vpn, notebook e celular corporativo, controle de acessos, verificação de postura de segurança, atualização dos equipamentos e ferramenta de apoio Office 365 (completo).

Ref	Titulo do Controle	Descrição do Controle	Nota	Comentários
A.7	**Seção 7 - Segurança em recursos humanos**		**4,6**	
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	5,0	
A.7.1.1	Seleção	Verificações do histórico devem ser realizadas para todos os candidatos a emprego, de acordo com a ética, regulamentações e leis relevantes, e deve ser proporcional aos requisitos do negócio, aos riscos percebidos e a classificação das informações a serem acessadas.	5,0	A empresa adota a verificação do histórico necessária que comprova que o candidato está habilitado para exercer a função através do recolhimento dos documentos admissionais. Como não há cargos com exigências especificas, a empresa não adota a verificação de habilitação em órgãos de classe (ex. CRC para contador).
A.7.1.2	Termos e condições de contratação	As obrigações contratuais com funcionários e partes externas devem declarar a sua responsabilidade e a da organização para segurança da informação	5,0	A empresa possui esta declaração evidente no contrato de trabalho, no termo de confidencialidade e na autorização de uso de dados pessoais. Também possui esta declaração evidente em contratos com terceiros. Os documentos passaram por revisão do departamento jurídico, e em caso de contratos com terceiros há revisão do departamento jurídico da empresa.

Ref	Titulo do Controle	Descrição do Controle	Nota	Comentários
A.7.2	Durante a contratação	Objetivo: assegurar que os funcionários e partes externas estão conscientes e comprei as suas responsabilidades pela segurança da informação	3,7	
A.7.2.1	Responsabilidades da direção	A direção deve requerer aos funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.	4,0	A direção através dos documentos admissionais relacionados a SI deixa evidente as responsabilidades dos funcionários e partes externas. Também reforça a necessidade de seguir estes regulamentos através de e-mail. Recomendação: incluir treinamentos em intervalos regulares com coleta de evidência para atender este controle de modo efetivo.
A.7.2.2	Conscientização, educação e treinamento em segurança da informação	Todos os funcionários da organização e, onde pertinente, as partes externas devem receber treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para suas funções.	2,0	A empresa adota boa comunicação em relação a SI no processo de integração do funcionário, mas não mantém um processo de conscientização formal ao longo do ano. No entanto, caso seja necessário adota a comunicação por e-mail de assuntos pertinentes a SI. Recomendação: promover a conscientização, educação e treinamento em relação a SI de forma regular com coleta de evidência.
A.7.2.3	Processo disciplinar	Deve existir um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação.	5,0	A empresa deixa evidente o processo disciplinar existe no contrato de trabalho, na documentação de integração e na integração com coleta de assinaturas. Recomendação: manter os funcionários informados através de treinamento para garantir a melhoria contínua.

Ref	Titulo do Controle	Descrição do Controle	Nota	Comentários
A.7.3	Encerramento e mudança da contratação	Objetivo: proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação	5,0	
A.7.3.1	Responsabilidades pelo encerramento ou mudança da contratação	As responsabilidades e obrigações pela segurança da informação que permaneçam válidas após o encerramento ou mudança da contratação devem ser definidas, comunicadas aos funcionários ou partes externas e cumpridas.	5,0	A empresa deixa evidente as responsabilidades em caso de encerramento ou mudança de contratação. Para os funcionários há comunicação da devolução dos equipamentos e revogação de acesso, e assinatura nos documentos formais de desligamento (o contrato possui clausula de confidencialidade). Para contratos com terceiros há clausula de confidencialidade nos documentos de contratação. Recomendação: no processo de desligamento reforçar que o funcionário não deve divulgar informações confidenciais.
A.9	**Seção 9 - Controle de acesso**		**4,0**	
A.9.1	Requisitos do negócio para controle de acesso	Objetivo: limitar o acesso à informação e aos recursos de processamento da informação	4,0	
A.9.1.1	Política de controle de acesso	Uma política de controle de acesso deve ser estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios	4,0	A empresa adota uma política de acesso que satisfaz esse controle de modo que: O controle de acesso inicial realizado pelo RH prevê o mínimo de acesso ao funcionário. As áreas determinam a extensão do acesso baseado nas funções que o funcionário executa. Recomendação: atualizar a política em intervalos regulares.
A.9.1.2	Acesso as redes e aos serviços de rede	Os usuários devem somente receber acesso as redes e ao serviço de rede que tenham sido especificamente autorizados a usar	4,0	A empresa possui controle de acesso rigoroso, de modo que o funcionário somente acessa o que foi autorizado. Recomendação: revisão de acessos versus autorização de acesso.

Ref	Titulo do Controle	Descrição do Controle	Nota	Comentários
A.9.2	Gerenciamento de acesso do usuário	Objetivo: assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços	4,0	
A.9.2.1	Registro e cancelamento de usuário	Um processo formal de registro e cancelamento de usuário deve ser implementado para permitir a atribuição dos direitos de acesso	4,0	Há um processo formal de registro e cancelamento de acessos através do sistema de chamado da empresa ou através de e-mail. Recomendação: concentrar a autorização através do sistema de chamado, pois o e-mail não é adequado para fins de auditoria uma vez que está restrito a caixa de entrada do funcionário.
A.18	**Seção 14 - Conformidade**		**4,0**	
A.18.1	Conformidade com requisitos legais e contratuais	Objetivo: evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas a segurança da informação e de quaisquer requisitos de segurança.		
A.18.1.4	Proteção e privacidade de informações de identificação de pessoal	A privacidade e proteção das informações de identificação pessoal devem ser asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.	4,0	A empresa adotou padronização de processos para atender a LGPD com auxilio de consultoria. Recomendação: manter atualizado os documentos através da revisão em intervalos regulares.