FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Marcelo Mendes Rocha

A SEGURANÇA DA INFORMAÇÃO EM ESPAÇOS DE COWORKING: UM ESTUDO DA EMPRESA PONTO BRASIL EM AMERICANA

Americana, SP

2017

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Marcelo Mendes Rocha

A SEGURANÇA DA INFORMAÇÃO EM ESPAÇOS DE COWORKING: UM ESTUDO DA EMPRESA PONTO BRASIL EM AMERICANA

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. Esp. Edson Roberto Gaseta.

Área de concentração: Segurança da Informação.

Americana, SP

2017

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

R574s ROCHA, Marcelo Mendes

A segurança da informação em espaços de coworking: um estudo da empresa Ponto Brasil em Americana. / Marcelo Mendes Rocha. – Americana, 2017.

52f.

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

Orientador: Prof. Esp. Edson Roberto Gaseta

1 Segurança em sistemas de informação I. GASETA, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Marcelo Mendes Rocha

A SEGURANÇA DA INFORMAÇÃO EM ESPAÇOS DE COWORKING: UM ESTUDO DA EMPRESA PONTO BRASIL EM AMERICANA

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, 14 de dezembro de 2017.

Banca Examinadora:

Edson Roberto Gaseta
Especialista
Faculdade de Tecnologia de Americana

Henri Alves de Godoy
Mestre
Faculdade de Tecnologia de Americana

Renato Kraide Soffner
Doutor
Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Agradeço primeiramente a Deus, sem que de forma singular me trouxe até aqui. Agradeço aos meus pais, Edson e Maria que dedicaram suas vidas para sempre proporcionar a melhor vida e educação possível, além de todo amor que meu deu forças para chegar até aqui.

À minha namorada Gisele, que sempre me apoiou, pelas experiências vividas e pela companhia dos longos finais de semana de estudo. Obrigado pelo seu carinho, alegria, sua atenção, sua vibração em minhas conquistas e teu ombro em cada momento difícil que você ajudou a atravessar. Sem você essa conquista não teria a mesma alegria.

Ao meu orientador, professor Edson, que me apoiou nesse desafio e acreditou no meu trabalho. Agradeço também por toda a paciência que teve comigo, pela constante ajuda durante as orientações, pelo conhecimento transmitido e pelo grande exemplo de ser humano que é.

A professora Maria Cristina, pela oportunidade, paciência, dedicação e credibilidade depositada em mim ao longo desse processo de graduação.

Ao grande amigo Rodrigo, por permitir o estudo de caso em sua empresa, pois sem isso jamais seria possível a conclusão desse trabalho.

Agradeço a todos que de uma forma ou de outra contribuíram para o desenvolvimento dessa etapa tão importante da minha vida.

DEDICATÓRIA

Dedico este trabalho a minha família, especialmente a minha mãe, Maria e minha namorada Gisele pela coragem, força e apoio dedicados, para seguir em busca da concretização dos meus objetivos.

RESUMO

O presente trabalho apresenta os ambientes de *coworking* e avalia se esses locais são capazes de garantir a segurança da informação. Foi conceituado o que são os espaços colaborativos e a importância para a economia atual, em especial para os *freelancers* e pequenas empresas. Explorou-se os princípios de Segurança da Informação para garantir a confidencialidade, integridade e a disponibilidade das informações com o intuito de proteção principal ativo organizacional. A partir da conceituação de espaços colaborativos e dos princípios de segurança da informação, verificou-se a necessidade de investigação, principalmente devido à taxa de crescimento dos escritórios compartilhados. Realizou-se um estudo de caso do *coworking* Ponto Brasil, em Americana, sendo elencado os principais pontos de segurança da informação para encontrar vulnerabilidades no local de estudo e sugerir melhorias para a proteção da informação das empresas e usuários do local. Com o levantamento dos dados, foi constatado que haviam melhorias a serem implementadas, mesmo que a infraestrutura do *coworking* já fosse funcional. Políticas de segurança da informação, nova configuração de rede, servidor de proxy, instalação de sistema de monitoramento, antivírus corporativo padronizado, contingência no sistema de rede elétrica foram sugeridos. Para finalização, foi verificado que existem pontos a serem melhorados no que diz respeito à segurança da informação e a visão de possui-la como um ativo estratégico para a empresa. Sugere-se que ações sejam tomadas para obter melhores práticas de proteção da informação e assim garantir sua qualidade, dais quais os resultados da implementação das mesmas poderão ser analisados em estudos futuros.

Palavras Chave: *Coworking;* Segurança da Informação; Riscos.

ABSTRACT

The present work presents the coworking environments and evaluates if these places are able to guarantee information security. It was conceptualized what are the collaborative spaces and importance for the current economy, especially for freelancers and small businesses. We explored the principles of Information Security to ensure the confidentiality, integrity and availability of information for the purpose of main organizational asset protection. Based on the conceptualization of collaborative spaces and the principles of information security, there was a need for research, mainly due to the growth rate of shared offices. A case study of coworking Ponto Brasil in Americana was carried out, and the main information security points were listed to find vulnerabilities in the study site and to suggest improvements for the protection of the information of the companies and users of the place. With the data collection, it was verified that there were improvements to be implemented, even if the coworking infrastructure was already functional. Information security policies, new network configuration, proxy server, installation of monitoring system, standardized corporate antivirus, contingency in the grid system have been suggested. For completion, it was verified that there are points to be improved with regard to information security and the vision of having it as a strategic asset for the company. It is suggested that actions be taken to obtain better information protection practices and thus guarantee their quality, from which the results of their implementation can be analyzed in future studies.

Keywords: *Coworking; Information Security; Risks.*

LISTA DE IMAGENS

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

Os ambientes de *coworking* surgiram nos EUA, em 2005, quando Brad Neuberg se juntou com seus amigos para criar um ambiente de trabalho diferenciado, mais flexível, no qual umas comunidades de profissionais de diferentes áreas compartilhassem o mesmo espaço e a mesma estrutura do escritório.

Atualmente são locais frequentados por profissionais de diferentes áreas que compartilham o mesmo espaço e vem chamando muita atenção de *freelancers* e microempresários que procuram outros meios para diminuir os custos fixos das organizações. De acordo com o site CWBE Coworking são “locais de estrutura qualificada e custo reduzido, os espaços compartilhados possibilitam aos profissionais a formação de uma rede de contatos especializada e fundamental para novas possibilidades.” (CWBE Coworking, 2017)

Em termos genéricos o *coworking* oferece aos usuários, chamados de *coworkers*: internet de ótima qualidade; energia elétrica; água e café; auditórios e salas de reuniões; serviços de limpeza; impressoras compartilhadas; recepcionista; entre outros, além do principal benefício do *networking* com um custo reduzido ou quase zero.

Mas, em termos de segurança da informação, os ambientes de *coworking* são realmente seguros? Os escritórios compartilhados atendem aos requisitos definidos no tripé da Segurança da Informação – SI?

Com o aumento da tecnologia e a mudança para o novo paradigma da economia, que considera o conhecimento empresarial como o fator de produção mais importante do século XXI, percebeu-se o aumento de ataques cibernéticos a grandes organizações que expôs publicamente informações privadas. O principal da segurança da informação é a proteção dos dados empresariais, garantindo a integridade, disponibilidade e confidencialidade.

O **objetivo geral** foi analisar a segurança no ambiente de *coworking* Ponto Brasil, localizado em Americana, interior do estado de São Paulo, considerando os princípios básicos da segurança da informação: garantia da confidencialidade, disponibilidade e a integridade da informação.

Foi definido como **objetivos específicos** do trabalho:

- Conceituar espaços de *coworking* e sua importância para a economia atual;
- Levantamento dos princípios básicos de Segurança da Informação;
- Análise da estrutura de SI no Ponto Brasil;
- Identificar as dificuldades enfrentadas pelo *coworking* estudado;
- Apontar recomendações e melhorias e criar políticas de proteção da informação com base no estudo do Tripé de SI.

O **método científico** utilizado foi a pesquisa bibliográfica envolvendo livros, artigos e publicações em revista e jornais, no intuito de obter o maior número de informações para construção do projeto.

Com a realização de um embasamento teórico consistente este trabalho auxiliará no estudo e na estruturação da Segurança da Informação em espaços compartilhados. Além disso, irá dar suporte à classe acadêmica voltada a proteção da informação na verificação da prática de *coworking* e ajudar em projeto e trabalhos futuros como facilitador na compreensão de áreas afins.

O crescimento do *coworking* é uma tendência do mundo atual, no qual redução dos custos e aumento da competitividade se tornou prioridade para as organizações. Porém é importante abordar a segurança da informação nesse contexto, pois a maior parte dos recursos utilizados são tecnológicos, gerando vulnerabilidades se não houver precauções.

No primeiro capítulo, descreve-se os espaços de *coworking*, sua história, sua estrutura e os principais benefícios desse novo modelo de negócio, além da comparação com as incubadoras e com a economia colaborativa. É apresentado os principais *coworkings* existentes no país.

Em seguida é feito uma abordagem do que é segurança da informação e seus principais pilares: integridade, disponibilidade e confidencialidade. É apresentado os princípios de gerenciamento de riscos e as diretrizes para implementação das políticas de segurança da informação.

No capítulo subsequente, é feito um estudo de caso no Ponto Brasil, analisando sua infraestrutura e apresentadas as vulnerabilidades encontradas e as melhorias para esses pontos.

Com a notoriedade que os espaços de *coworking* ganharam nos últimos tempos, surge uma indagação: esses espaços são realmente seguros? Possuem políticas de segurança? Preocupam-se com a integridade digital de seus *coworkers*?

1. OS ESPAÇOS DE *COWORKING*

A essência do *coworking* vem do Séculos XX, dos antigos *caffés littéraires* da Europa que funcionavam como ponto de encontro e estudos, um local de reuniões e idealizações. Já o termo aparece em 1999, com autoria de Bernie DeKoven que desenvolveu um novo tipo de plataforma computacional para apoio em reuniões de negócios, apresentando os pontos mais importantes baseado no princípio de *'working together as equals*[1]*'*. (Soares e Saltorato, 2015)

O site DESK Coworking informa que o *coworking* surgiu em meados de 2005 com a ideia de Brad Neuberg de "criar uma comunidade de profissionais que compartilhassem do mesmo espaço de trabalho e pudessem aproveitar o que há de melhor na estrutura de um escritório". (DESK Coworking, 2017) Para Gandini, o *coworking* representa uma:

> "terceira via de serviços, sendo um modelo intermediário entre o trabalho tradicional, delimitado em uma comunidade homogênea, e uma vida profissional independente, como *freelancer*, que possui uma característica de liberdade e independência, onde as atividades são desempenhadas em casa, no isolamento". (Revista Espacios, 2015)

A principal diferença dos escritórios comuns para os escritórios compartilhados é "o foco em uma comunidade e a partilha de conhecimentos. São organizações e profissionais diferentes partilhando dos mesmos valores: comunidade, abertura e independência". (DOULAMIS, 2013; SPINUZZI, 2012).

De acordo com dados do Censo Brasil 2017, realizado pelo *site coworkingbrasil.org* há, atualmente:

- 810 espaços ativos conhecidos em fevereiro/2017;
- Total de 210 mil pessoas que movimentam mensalmente os espaços, para trabalhos, reuniões e/ou participar de eventos;
- Em 2016, foi declarado um faturamento de R$ 82 milhões;

[1] **Tradução do autor:** "Trabalhando juntos igualmente". MAGID, L. J. Outlining brings meeting to order. Los Angeles Times, 29 mar. 2000.

- Os espaços compartilhados geram um total de: 2326 empregos diretos (contratados diretamente) e 1174 empregos indiretos (*freelancers* e autônomos).

O aumento da comunidade de *coworkers* se dá pelo crescimento do número de profissionais *freelancers* e autônomos, além de empreendedores e profissionais da aréa de tecnologia que buscam locais para o aumento da produtividade, compartilhamento de informações, melhores custos e ótima infraestrutura. (DOULAMIS, 2013).

Munhoz descreve os espaços de *coworking* como:

> "um ambiente dividido entre pessoas com funções bem distintas que, além da estrutura física, também compartilham seus custos de locação. O objetivo é criar um ambiente propício ao relacionamento, troca de experiências, valores sinergia e networking. Em ambientes como estes, as start-ups discutem ideias e geram novas oportunidades, proporcionando a criação de novos negócios". (Munhoz, 2015, p. 04)

O *coworking* hoje se apresenta como uma forma de reflexão e recriação do ambiente de trabalho tradicional. (COWORKINGBRASIL.ORG, 2017)

Em artigo publicado na Revista Espacios, Oliveira, Freitas Filho e Lanzer (2016) definem que as principais áreas do conhecimento identificadas nos principais escritórios compartilhados são: negócios sociais, *design*, *start-ups*, educação, moda, empreendedorismo, advocacia, arquitetura, entre outros.

Conforme Munhoz (2013, p.10) os principais benefícios de fazer parte da rede colaborativa do *coworking* são:

- Suporte financeiro: custo baixo com boa estrutura e diminuição dos custos fixos com aluguel, energia elétrica, internet, entre outros;
- Networking, interação comunitária, troca de experiências e ambiente colaborativo;
- Salas de reunião;
- Espaço para eventos;
- Internet sem fio (alta velocidade);
- Salas de treinamento;
- Impressora multifuncional;
- *Lounge* (espaço de relaxamento), etc.

Para Soares e Saltorato (2015, p. 71), os principais pontos negativos em escritórios compartilhados são: a questão de inter-relacionamentos e a gestão do ambiente. Além disso, existem questões como a falta de privacidade, possível dificuldade de concentração e a pressão para fazer networking e a vulnerabilidade das redes *Wireless*. (LEFORESTIER, 2009)

1.1 Economia Colaborativa

O conceito de Economia Colaborativa está contribuindo para o crescimento dos espaços de escritórios compartilhados.

De acordo Owyang, Tran e Silva (2013, p. 04) a economia colaborativa pode ser definida como "um modelo econômico onde a propriedade e o acesso são compartilhados entre corporações, startups e pessoas. Isso resulta em eficiências de mercado que oferecem novos produtos, serviços e crescimento de negócios"[2]

Pouco explorada no mundo acadêmico, a expressão é conhecida como consumo colaborativo, empréstimos, trocas, produção colaborativa (P2P ou *peer-to-peer*) e está crescendo e se tornando popular no mercado mundial.

A economia colaborativa é um complemento do *coworking* pois ambas possuem o mesmo objetivo de compartilhar e socializar.

Daunoriené (2015) explica que, na economia popular, para a posse de algo é necessário o pagamento financeiro, enquanto na economia compartilhada, é criado um valor temporário para os bens ou serviços.

A economia colaborativa é popularmente conhecida nas práticas diárias da população como pedir caronas, emprestar algo para alguém ou de alguém, hospedar parentes e conhecidos, usar bibliotecas e transporte coletivo.

[2] Texto original: "is an economic model where ownership and access are shared between corporations, startups, and people. This results in market efficiencies that bear new products, services, and business growth" OWYANG, Jeremiah; TRAN, Christine; SILVA, Chris. **The collaborative economy**. Altimeter, United States, 2013, p. 04

1.2 Diferença entre *Coworkings* e Incubadoras

Coworking é uma comunidade de independentes. Oferece uma variedade de níveis de adesão para uma comunidade de pessoas de mentalidade semelhante em um espaço central de reunião. Apela para *freelancers*, trabalhadores remotos, proprietários de pequenas empresas e viajantes. É para a pequena equipe cujo trabalho não requer muito mais do que uma mesa e uma conexão à *Internet.*

Já as incubadoras de empresas são um dos fomentos para o empreendedorismo. Existem diversos tipos, serviços oferecidos e vantagens de ser uma empresa incubada. Por meio do apoio das Incubadoras, as empresas podem contar com suporte de desenvolvimento e treinamento necessários até que esta adquira estrutura e experiência suficiente para dar continuidade a seu negócio.

As incubadoras de empresas têm como objetivo apoiar o desenvolvimento de empresas oferecendo um conjunto de recursos e serviços de apoio. Elas buscam assessorar pequenos e médios empreendedores interessadas em abrir um negócio (SEBRAE, 2017).

Considerada como uma instituição de apoio, para garantir seu funcionamento são necessárias parcerias diversificadas. É um conjunto de instituições para manter a incubadora em prol do empresário. É uma rede de cooperação que apoia e atrai parceiros governamentais, tecnológicos e empresariais.

Na sua infraestrutura as incubadoras buscam a comercialização dos produtos gerados pelas empresas, e diversos mercados, os objetivos irão variar de acordo com o tipo de incubadora e do produto/serviço proposto pela empresa incubada.

Algum dos serviços oferecidos pelas incubadoras são: telefonia e acesso à internet, recepcionista, segurança, reprografia, assinatura de jornais e revistas, assessoria gerencial, contábil, jurídica, apuração e controle de custo, gestão financeira, comercialização, exportação e para o desenvolvimento do negócio (SEBRAE, 2017).

As principais diferenças entre os *coworkings* e as incubadoras são, de acordo com Barbosa (2015, p. 10), conforme mostrado na Tabela 1.

Tabela 1: Diferenças entre *coworkings* e incubadoras:

Coworking	**Incubadoras**
Criado para todos os tipos de empresa, de qualquer setor econômico, sem restrição de tamanho e tempo de funcionamento;	Para pequenas empresas no início das suas atividades;
Objetivo inicial: dinamizar o ambiente de trabalho, em busca de um local comunitário e redução de isolamento;	Criada para aumentar a possibilidade de sobrevivência, diminuindo o índice de morte prematura empresarial;
Relação flexível baseada nas necessidades individuais.	Relação de longo prazo.

Fonte: adaptado de Barbosa, 2015, p. 10

1.3 Principais espaços de *Coworking*

Alguns dos principais espaços de *coworking* estão apresentados abaixo:

1.3.1 *Google* Campus SP

O campus da *Google* em São Paulo, localizado na zona sul, foi inaugurado em junho de 2016. É um espaço gratuito, voltado ao empreendedorismo, especial para quem quer iniciar um novo negócio ou se conectar com outras *start-ups.* Foi o primeiro espaço da Google na América e, hoje, já pode ser encontrado em lugares como Londres, Seul, Madri, entre outros.

O prédio de São Paulo possui mais de 7 mil membros inscritos que podem utilizar o espaço todos os dias das 09h00 às 19h00: rede *Wireless* gratuita, auditórios com capacidade para 100 pessoas, salas de reuniões, mesas, *lounges*, entre outros benefícios, conforme representado pela Imagem 1.

Além disso, a *Google* oferece um programa de mentoria para *startups*, com duração de seis meses, no qual os funcionários da empresa desenvolvem projetos de auxílio às empresas com o objetivo de desenvolvimento e expansão.

Imagem 1: *Google* Campus SP

Fonte: Campus São Paulo

1.3.2 *Impact Hub* São Paulo

Possuindo uma rede global com mais de 15000 membros em mais de 90 locais, o *Impact Hub* é um laboratório para inovação. É, ao mesmo tempo, um *coworking*, uma incubadora, uma rede de negócios e um centro comunitário para empreendimentos sociais.

Aberto em 2008, possui vários atualmente vários projetos, como a *Hub* Escola, a Consultoria e o *Fellowship* (programa de incubação), além de um segundo espaço localizado na Vila Madalena. A comunidade do *Impact Hub* São Paulo é composta por negócios e projetos sociais a nível local e global. Os membros são empreendedores, investidores sociais, *freelancers*, consultores, empreendedores, entre outros, que usufruem de uma plataforma global de conexão e possuem acesso à acervos, treinamentos e suporte; utilizam os espaços para encontros e trabalho; e participam

de atividades como exposições, palestras, debates, *workshops*, etc, conforme mostrado na Imagem 2.

Imagem 2: *Impact Hub*

Fonte: Impact HUB

1.3.3 Elo *Coworking*

O Elo *Coworking* é um Escritório Compartilhado com moderna e ampla infraestrutura na cidade de Belo Horizonte, Minas Gerais. Está localizado no bairro Belvedere e possui agências bancárias, estacionamento, restaurantes, correios, lanchonetes, supermercados e shopping centers ao redor.

A pessoa contrata um dos planos oferecidos e pode ter a disposição todas as facilidades de um grande escritório, em ótimo ambiente empresarial, sem nenhum investimento.

Os principais benefícios, conforme descrito no site http://elocoworking.com.br/ para fazer parte do Elo *Coworking* são:

- Não possui a burocracia dos contratos de aluguel;

- Não possui altos custos fixos mensais, nem a administração de despesas como aluguel, condomínio, além de diversas taxas e serviços;
- Não possui contrato por tempo, permitindo maior liberdade e flexibilidade;
- Não faz investimentos em móveis, reformas e estrutura tecnológica, que imobilizam seu capital;
- Ambiente altamente profissional;
- Interage com profissionais de vários segmentos, em excelente ambiente empresarial, gerando ampla rede de contatos e até negócios;
- Excelente infraestrutura e localização e privilegiada.

2. PRINCIPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

O uso de redes de computadores, *notebooks* e *internet* possibilitou a melhoria da produtividade para os funcionários e organizações. A Era da Informação, comumente chamado o novo paradigma econômico, alterou o foco das organizações: o que antes era considerado maior valor, os meios de produção, se tornou secundário, sendo substituído pela produção de informação e conhecimento; maior ativo empresarial na sociedade atual.

Fontes (2006) afirma que a informação é um recurso que move o mundo e é mais que um conjunto de dados. O processo de transformar dados em informação é converter algo que tem baixo significado prático em um recurso fundamental para a vida pessoal ou profissional. Complementando, a informação é um ativo essencial para os negócios de uma organização e necessita ser adequadamente protegida. Isto é essencialmente importante no ambiente empresarial, cada vez mais interconectado e competitivo.

Como consequência dessas mudanças, um grande contingente de pessoas tenta usar as informações confidenciais para obter vantagens de pessoas ou empresas. Nesse contexto, é necessário estudar o que é segurança da informação e seus princípios. Beal (2005) define a segurança da informação como “o processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade”.

De acordo com Marciano e Lima-Marques (2006), Segurança da Informação é:

> “um fenômeno social no qual os usuários (aí incluídos os gestores) dos sistemas de informação têm razoável conhecimento acerca do uso destes sistemas, incluindo os ônus decorrentes expressos por meio de regras, bem como sobre os papéis que devem desempenhar no exercício deste uso.” (Marciano e Lima-Marques, 2006, p.95)

Até o ano de 2002, toda a responsabilidade de proteger informações corporativas era atribuída ao departamento de TI. Não havia nenhum procedimento especial e os incidentes eram analisados caso a caso, além da segurança de TI possuir o status de custo, não de um recurso ou investimento necessário para diminuir

os prejuízos causados por imprevistos que paralisam as operações da empresa. Assim como é a preocupação com os recursos financeiros e materiais, é imprescindível que as organizações criem mecanismos para proteger a informação e sua utilização deve ser pautada por normas e procedimentos. (Turban, 2010)

Com isso é imperativo que os profissionais envolvidos com a gestão da informação e proteção de documentos sigilosos se atentem com a guarda, a preservação, o controle e acesso, sempre com o intuito de encontrar novas formas e novos processos que garantam os princípios da autenticidade, confiabilidade, documento ser físico ou virtual. Nesse sentido, as instituições são responsáveis pelo tratamento das informações e princípios que norteiam as ações para proteção institucional. (SFREDDO E FLORES, 2012)

De acordo com a ABNT NBR ISO/IEC 27002:

> "A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização são atendidos." (ABNT NBR ISO/IEC 27002, 2013, p. 04)

A publicação ISO/IEC 27000 (2014, p.17) define as ameaças como: "causa potencial de um incidente indesejado, o que pode resultar em danos a um sistema ou organização"[3].

Nos subcapítulos abaixo, será apresentado os princípios básicos de SI, seus conceitos e premissas, além da importância dos mesmos para as organizações.

2.1 Conceitos gerais

Os princípios fundamentais da segurança da informação têm como finalidade diminuir os riscos a que estão sujeitos os ativos de uma organização. Essa compreensão precisa ser complementada pelos conceitos fundamentais de SI.

---

[3] Texto original: *"potential cause of an unwanted incident, which may result in harm to a system or organization"* ISO/IEC 27000, 2014.

Ramos (2008) apresenta os elementos que são usados nas definições de incidentes de segurança da informação:

- **Ativos de informação:** a informação propriamente dita, toda a infraestrutura ligada à informação e as pessoas que têm acesso a informação;
- **Valor dos ativos:** é a importância para a empresa que pode ser medida pelo custo de reposição, pelo prejuízo com a perda ou ainda pelo comprometimento da imagem da organização;
- **Requerimentos de segurança:** ações necessárias para diminuir a probabilidade de um risco se efetivar;
- **Controles de segurança:** ações e procedimentos que atendem aos requerimentos de segurança e visam eliminar as vulnerabilidades dos ativos de informação;
- **Vulnerabilidade:** é uma fraqueza de procedimento, software ou hardware, que permite que um hacker invada um computador ou uma rede de computadores, obtendo acesso a recursos nestes ambientes. Uma vulnerabilidade pode ser caracterizada pela ausência ou fraqueza de uma salvaguarda que pode ser explorada;
- **Ameaça:** pode ser compreendida como a ausência ou falhas em mecanismos de proteção que não previnem algum perigo potencial para a informação ou para os sistemas. A ameaça ocorre quando há a tentativa de exploração de uma vulnerabilidade. A entidade que obtém vantagem da vulnerabilidade é conhecida como “agente”;
- **Risco:** é a probabilidade de uma ameaça se concretizar combinada com os impactos que ela trará. É a principal métrica gerencial da segurança da informação: quanto maior a probabilidade de uma ameaça se concretizar e o impacto associado a ela, maior o risco.

Dentro desse contexto, define-se que a confidencialidade está ligada ao processo de classificação da informação e à concessão de direito de acesso à informação. Os direitos de acesso são disponibilizados quanto à necessidade de acesso e à classificação da informação.

Já a integridade dos dados está ligada ao controle de acesso e à qualidade dos dados. Um dado confiável é aquele que está integro e correto e essa é a base do processo de tomada de decisões. Sem dados confiáveis, toda e qualquer decisão poderá ser tomada de forma errada, causando prejuízos à organização

O princípio da disponibilidade afirma que a informação deve estar disponível sempre que for solicitada por um usuário com direito de acesso. A maior dificuldade para se manter a disponibilidade da informação está na manutenção da redundância dos recursos necessários para o armazenamento, transmissão e acesso. A rápida resposta à perda de dados pode diminuir os prejuízos causados pela parada dos sistemas de informação.

2.2 Tripé de Segurança da Informação

A segurança da informação apresenta três princípios básicos, conhecido como tripé de SI, que são: confidencialidade, integridade e disponibilidade. Um resumo dos estudos e das definições feitas por Harris (2008) e Tittel and Stewart (2003) é apresentado abaixo:

1. **Confidencialidade:** O principal objetivo da confidencialidade é a garantia de que o nível de segredo de uma informação será reforçado pelo processamento dos dados e pela prevenção de exposição não autorizada. Os ataques à confidencialidade podem ocorrer pelo monitoramento da rede, pelo roubo de arquivos de senhas ou engenharia social (quando alguém engana outra pessoa para obter acesso não autorizado a informações). É possível a melhoria da confidencialidade, utilizando como principais ações: a) criptografia dos dados armazenados e transmitidos por uma rede de dados; b) definição de quem tem direito de acesso para cada informação e quais os direitos concedidos; c) classificação da informação; d) treinamento dos usuários no uso correto da informação e dos dispositivos de acesso à informação. A garantia da confidencialidade é uma das tarefas de maior dificuldade de implementação, pois em suas ações são levados em conta todos os elementos que fazem parte da comunicação da informação, o valor da informação para a organização e os impactos causados pela divulgação indevida.

2. **Integridade:** a informação íntegra é aquela que não foi alterada de forma indevida ou não autorizada. É possível manter integridade da informação garantindo a precisão e confiabilidade fazendo com que o hardware, o software e os mecanismos de comunicação trabalhem em conjunto para manter e movimentar os dados corretos para seus destinos sem alterações inesperadas. Os sistemas e a rede devem ser protegidos de interferência externa e contaminação para garantir que invasores (ou que erros cometidos pelos usuários) não comprometam a integridade dos dados. Quando um hacker insere um vírus a integridade do sistema é comprometida, podendo afetar negativamente toda a organização. O controle estrito de acesso, a detecção de intrusão, entre outros métodos, pode combater essas ameaças.
3. **Disponibilidade:** sistemas e redes de computadores apresentam uma adequada capacidade de desempenhar suas funções de maneira previsível e em um nível de desempenho aceitável. Eles devem ter a habilidade de se recuperar de rompimentos do funcionamento de modo a não afetar a produtividade da empresa. Pontos únicos de falha devem ser evitados e, quando necessário, devem ser instaladas políticas de backup e mecanismos de redundância. A disponibilidade é a garantia de que a informação estará acessível quando necessária, e relaciona-se a toda infraestrutura ligada à informação e aos serviços prestados por ela: acesso, trânsito e armazenamento.

Porém, além de se preocupar com esses três aspectos, é necessário ficar atento ao processo de comunicação da empresa, conforme Beal afirma:

> "Problemas como a alteração fraudulenta de documentos em trânsito e disputas sobre a origem de uma comunicação ou o recebimento de uma informação transmitida precisam ser equacionados, levando à necessidade de estabelecer alguns objetivos adicionais relativos à segurança da comunicação." (BEAL, 2005, p.2)

Segundo Sfreddo e Flores (2012, p. 163), a confidencialidade é a garantia de que as informações estão acessíveis apenas para usuários permitidos, a integridade protege as informações de serem modificadas ou adulteradas e a disponibilidade assegura que os usuários com autorização tenham acesso às informações de maneira protegida sempre que for necessário.

Para garantir a segurança dos ativos de informação contra perda, furto e alteração, divulgação ou destruição indevidas, além de outros problemas que podem alterá-los, é necessário a adoção de controles de segurança – medidas de proteção que abrangem uma grande diversidade de iniciativas, indo dos cuidados com os processos de comunicação â segurança de pessoas, mídias e componentes de TI. (BEAL, 2005, p.10)

2.3 Gerenciamento de riscos em SI

O risco é uma métrica utilizada em Segurança da Informação para mensurar o impacto das ameaças em caso de concretização.

Com base na NBR ISO/IEC 27001, é conveniente que as análises de riscos "avalie as consequências potenciais que podem resultar se os riscos identificados; avalie a probabilidade realística da ocorrência dos riscos identificados e determine os níveis de risco". (ABNT NBR ISO/IEC 27001, 2013, p. 08) Os resultados dessas avaliações devem obter resultados para orientar e determinar as ações dos gestores de forma apropriada, priorizando o gerenciamento de riscos.

De acordo com Scudere (2006) a análise de riscos pode ser dividida em seis dimensões, tais como: 1) planejamento de ações e criação de estratégias, 2) criação de procedimentos para identificação dos riscos, 3) qualificação das vulnerabilidades e ameaças, 4) quantificação do nível de risco, 5) elaboração de procedimentos que determinem o impacto e o tempo de resposta, 6) definição de procedimentos para monitoramento/controle dos riscos e as ações para minimizá-los.

É necessário que o exame feita estime a magnitude do risco e compare-os com os critérios e consequências para determinar o valor que esse risco representa para a organização. Além disso, devem ser realizados periodicamente para verificar se houve alterações nos requisitos de S.I. e na métrica da situação de risco. Para finalizar, devem ser feitos de forma ordenada para a geração de resultados comparáveis e reproduzíveis e possuir um escopo claro, objetivo, conciso e eficaz.

As principais opções para o tratamento dos riscos, listados na ABNT NBR ISO/IEC 27001 são:

1) Selecionar as opções de tratamento conforme os resultados das avaliações de risco;
2) Determinar a aplicação dos controles apropriados para redução de riscos;
3) Preparação de plano de tratamento de riscos;
4) Declaração de aplicabilidade dos com os controles e justificativas para implementação;
5) Obter a aprovação dos responsáveis para o planejamento de tratamento de riscos;
6) Manter toda a informação documentada (ABNT NBR ISO/IEC 27001, 2013, p. 06 e 07)

Para o tratamento dos riscos é feita a seleção de controles apropriados que serão sejam selecionados e implementados para atendimento dos requisitos identificados pela análise de riscos, com o intuito de reduzi-los a um nível aceitável. A seleção dos controles:

> "depende das decisões da organização, baseadas nos critérios para aceitação de risco, nas opções para tratamento do risco e no enfoque geral da gestão de risco aplicado à organização e convém que também esteja sujeito a todas as legislações e regulamentações nacionais e internacionais, relevantes." (ABNT NBR ISO/IEC 27002, 2013, p. 5)

Esses controles devem garantir que os riscos sejam reduzidos a um nível aceitável, considerando os requisitos da legislação vigente, os objetivos da organização, o custo de implementação proporcional à probabilidade de danos.

2.4 Política de segurança da informação

O objetivo da criação de Políticas de Segurança da Informação nas organizações é o de orientar e apoiar a alta administração, considerando os objetivos dos negócios e a proteção da informação.

A NBR ISO/IEC 27002 (2013, p. 08) define como objetivo das políticas de SI "prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes."

Para Silva Netto e Pinheiro da Silveira (2007, p. 380) "a política de segurança e a conscientização dos usuários são algumas das formas de se controlar a segurança na camada humana".

Casanas e Machado (2001, p. 05) defendem que:

> “a definição e adoção de uma política de segurança de rede, torna-se fundamental, pois coloca a informática sob controle, evitando perda de produtividade, aumentando a disponibilidade dos sistemas e protegendo as informações contra qualquer tipo de uso indevido” (Casanas e Machado 2001, p. 05)

As principais diretrizes para implementação, de acordo com a NBR ISO/IEC 27002 são:

1) Definir a segurança da informação, suas metas globais, escopo e importância para a organização;
2) Comprometimento da alta direção, considerando que as metas e princípios da segurança da informação estão alinhada com os objetivos e estratégias do negócio;
3) Estabelecer os objetivos de controle e os controles para o gerenciamento de riscos;
4) Divulgação das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para todos os funcionários de forma clara;
5) Definir os responsáveis e as responsabilidades gerais e específicas no gerenciamento de riscos;
6) Análise crítica constante das políticas de Segurança da Informação para verificar a eficácia e adequação;
7) Inclusão da avaliação de oportunidades visando a melhorias das políticas implementadas. (ABNT NBR ISO/IEC 27002, 2013, p. 08, 09 e 10)

3. ESTUDO DE CASO: ANÁLISE DO PONTO BRASIL

O objetivo desse trabalho foi fazer um estudo da estruturação da segurança da informação em escritórios compartilhados, visando identificar se nesses locais há a garantia da confidencialidade, disponibilidade e a integridade da informação. Para isso, escolheu-se o *coworking* Ponto Brasil, localizado em Americana, interior do estado de São Paulo.

Abaixo apresenta-se a história do local, a infraestrutura física e de redes, as vulnerabilidades encontradas e as sugestões de melhoria pelo autor.

3.1 O Ponto Brasil

No ano de 2011, surgiu na mente de Rodrigo Lopes Jorge, fundador do Ponto Brasil, ideia de construir um escritório diferente, reunindo diferentes profissionais no mesmo ambiente dividindo as despesas entre si. Após pesquisas, verificou-se que esse tipo de local era um modelo comum nos EUA, com adeptos no espaço nacional.

Assim, Rodrigo visitou espaços semelhantes em São Paulo para melhor entendimento do conceito e iniciou o projeto, que se concretizou a partir de janeiro de 2014, se tornando o primeiro *coworking* de Americana/SP, oferecendo aos usuários um espaço amplo localizado próximo à Av. Brasil, das principais regiões da cidade.

Com uma área de aproximadamente 1200 m², dos quais 300 m² são construídos, possui amplo estacionamento, salas individuais, cozinha montada, espaço gourmet, auditório, sala de reuniões e estações de trabalho fixa e compartilhada, conforme mostrado nas abaixo nas imagens 3, Imagem 4, Imagem 5, Imagem 6 e Imagem 7. O horário de funcionamento é das 8h00 às 22h00, de segunda à sexta. A abertura aos finais de semana está condicionada aos eventos agendados. Está localizado atrás do shopping Smart Mall, da Av. Brasil de Americana/SP (Rua Amélio Ettore Gobbo, 113), próximo a agências bancárias, restaurantes, postos de combustível, supermercado e escolas técnicas, conforme mostrado na Figura 1.

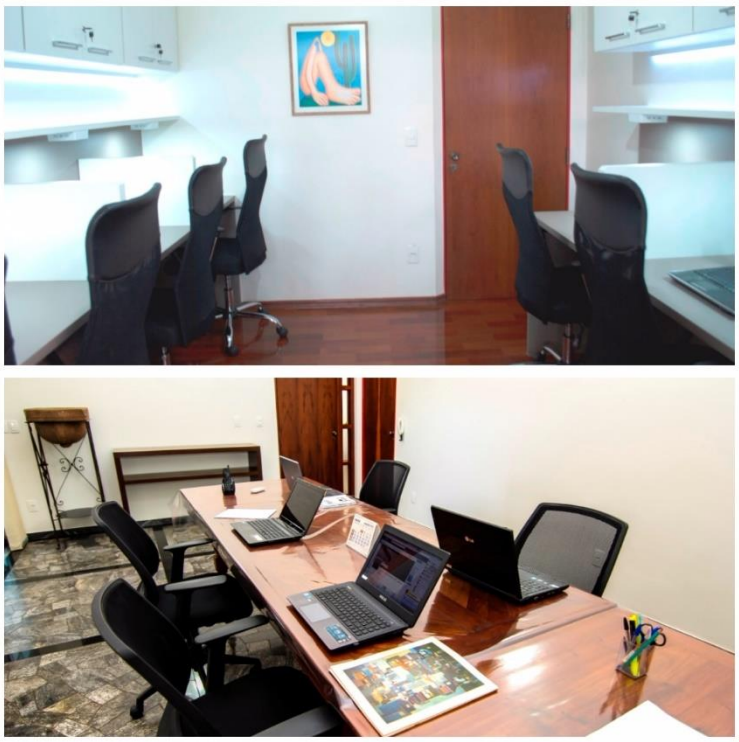
Imagem 3: Fachada e Estacionamento do Ponto Brasil

Fonte: Ponto Brasil

Imagem 4: Recepção e Lounge

Fonte: Ponto Brasil

Imagem 5: Estações fixas e compartilhadas



Fonte: Ponto Brasil

Imagem 6: Sala individual

Fonte: Ponto Brasil

Imagem 7: Sala de reunião e auditório

Fonte: Ponto Brasil

Figura 1: Localização Ponto Brasil – Google Maps

Fonte: Ponto Brasil

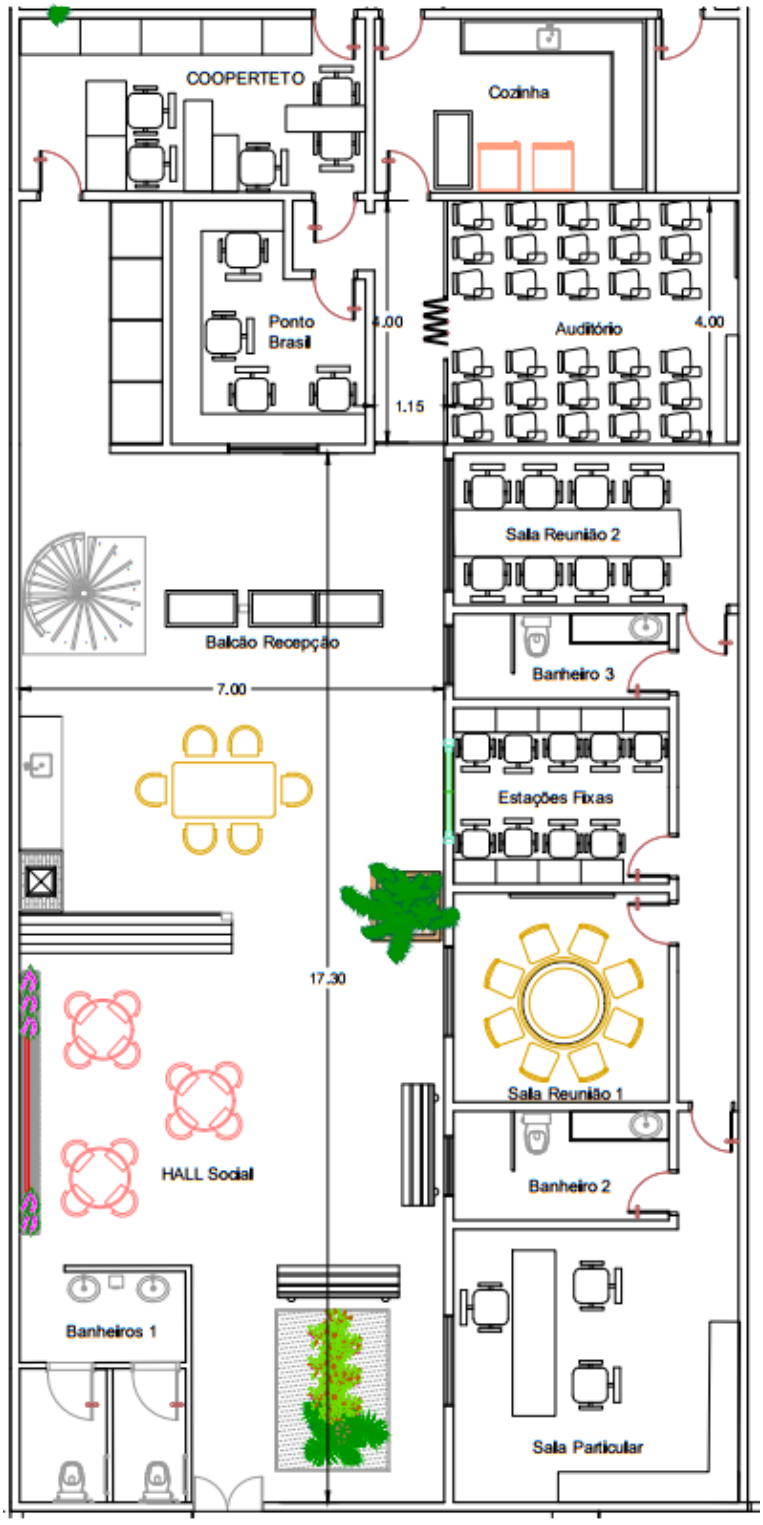
Atualmente, estão instaladas no Ponto Brasil as seguintes empresas de forma fixa: Cooperteto, Otimize Gráfica e Devi Tecnologia. Conforme constatado com o proprietário da Devi Tecnologia, Lucas Souza, a decisão de estar em um *coworking* veio em um momento de crise e reestruturação na empresa, com um fluxo de caixa

abarrotado de contas a pagar e carteira de clientes pequena. Em pesquisas na internet para novo local com aluguel mais acessível, Lucas encontrou o Ponto Brasil que contemplava em um mesmo valor: aluguel, internet, gastos com agua e energia elétrica, café e uma ótima estrutura e localização. Com essa mudança foi possível focar nos objetivos empresariais e se reestabelecer no mercado de softwares.

3.2 Infraestrutura física e de redes

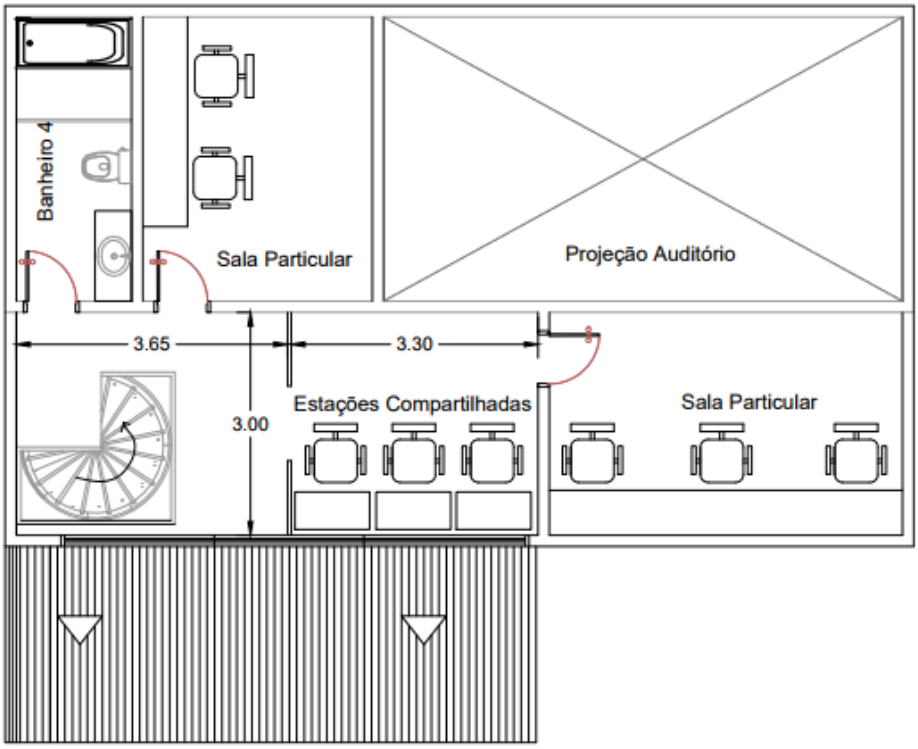
O local estudado possui uma área de aproximadamente 1200 m², dos quais 300 m² são construídos. O espaço é dividido em estacionamento, salas individuais, cozinha montada, espaço gourmet, auditório, sala de reuniões e estações de trabalho fixa e compartilhada. O acesso é permitido a qualquer visitante pelo Hall social e lounge. O térreo possui o balcão da recepcionista, a empresa Cooperteto, o auditório, as estações compartilhadas e fixas e as salas de reunião e auditório. Os banheiros são divididos por numeração, sendo o Banheiro 1, para uso comum e localizado próximo à entrada, O Banheiro 2 e Banheiro 3 são disponibilizados para os *coworkers*. O local ainda dispõe de uma cozinha e refeitório para os usuários. No segundo andar, está localizado a Gráfica Otimize, a sala particular utilizada pela Devi Tecnologia, o Banheiro 4, de uso público, e algumas estações compartilhadas. A empresa não possui monitoramento por câmeras de segurança, nem porteiros ou responsáveis pela vigilância. O único dispositivo de segurança utilizado no *coworking* é o alarme acionado no período noturno. Abaixo, na Figura 2, está apresentado a planta baixa do térreo do Ponto Brasil e, na Figura 3, a planta referente ao segundo andar.

Figura 2: Planta baixa 1° andar Ponto Brasil



Fonte: disponibilizado pelo proprietário do Ponto Brasil

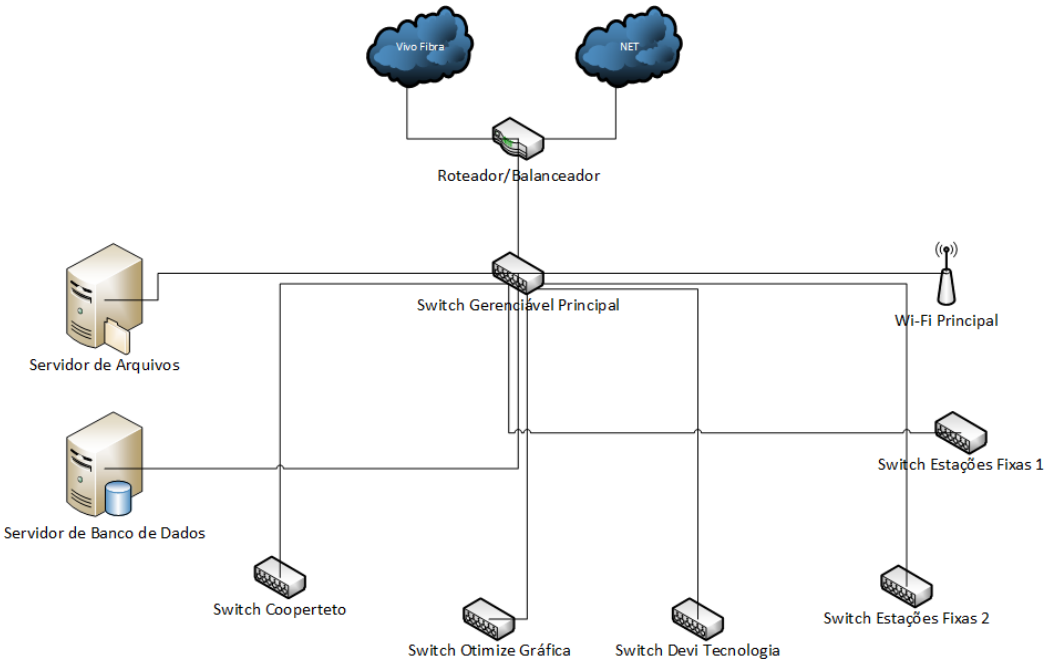
Figura 3: Planta baixa 2° andar



Fonte: disponibilizado pelo proprietário do Ponto Brasil

A estrutura de redes está configurada com a topologia de redes do tipo estrela, na qual todos os dispositivos (computadores e equipamentos) estão conectados à um *switch* principal (equipamento comutador encarregado de retransmitir os dados para todas as estações). A rede possui dois *links* de *internet*, utilizando os serviços da Vivo Fibra e Net com velocidade de 100 mb cada um, conectados ao roteador (responsável pelo gerenciamento das rotas da rede) e ao balanceador, que define o *link* de *internet* a ser utilizado. Cada uma das salas do Ponto Brasil possuem um sub-*switch*, utilizados para conexão cabeada dos equipamentos. Além disso, possui dois servidores, um de banco de dados e outro de arquivos, utilizados pelos sistemas do Ponto Brasil e da empresa Cooperteto. A conexão *wi-fi* é disponibilizada por um único ponto de acesso, que abrange boa parte do ambiente. A estrutura de redes é apresentada na Figura 4 abaixo.

Figura 4: Projeto de rede atual do Ponto Brasil



Fonte: elaborado pelo autor

Pode se considerar que a rede utilizada é funcional, porém desprotegida e vulnerável às ameaças, pois qualquer dispositivo conectado tem acesso não monitorado à rede.

3.3 Vulnerabilidades encontradas

Após estudo e análise do Ponto Brasil, foram listados os seguintes problemas e dificuldades:

- **Inexistências de políticas de SI:** Considerado uma das principais falhas na maioria das organizações, foi constatado que no Ponto Brasil esse problema se repete;
- **Danos com vírus e *malware*:** Segundo um relatório da Symantec, 42.4 milhões de usuários foram afetados por cibercrimes no Brasil em 2016 e a tendência é que essas invasões aumentem cada vez mais devido a constantes criações de novas ameaças. Verificou-se que no Ponto Brasil não é utilizado nenhum sistema de defesa e os usuários estão totalmente desprotegidos. As consequências podem ser graves em casos de violação, podendo expor e prejudicar seriamente as empresas do *coworking*;

- **Ameaças Internas:** Por se tratar de um espaço aberto para utilização de qualquer indivíduo, podem ocorrer casos de má fé no qual pessoas se infiltram para observar e fraudar as organizações do local, pois passam a ter acesso aos dados da empresa, plena ou parcialmente;
- **Energia elétrica:** Não é recorrente as quedas de energia no Ponto Brasil, porém, quando há incidência o problema se estende por horas e não há sistemas de contingência, como *nobreaks* ou geradores, afetando assim vendas, faturamento, atendimento, entre outros;
- **Falhas humanas:** Nesse quesito é importante salientar a falta de preparo das pessoas em navegar na internet, senhas com baixa complexidade, remoção de dados por acidente, gravações em dados existentes, desinstalação e alteração de arquivos importantes para o sistema, causando riscos a rede de dispositivos;
- **Ausência de *backup* regular:** No *coworking* estudado não há nenhum tipo de backup configurado, podendo levar a prejuízo caso os dados forem perdidos/danificados;
- **Monitoramento e segurança:** conforme descrito no tópico Infraestrutura física e de redes, o Ponto Brasil não possui sistema de segurança, câmeras ou porteiros e vigilantes. O único dispositivo utilizado é o alarme noturno.

Tabela 1: Vulnerabilidades do Ponto Brasil e principais riscos oferecidos

Vulnerabilidades	Principais Riscos
Inexistências de políticas de SI	• A falta de normatização deixa aberto ao bom senso dos usuários a organização e a utilização dos equipamentos disponibilizados.
Danos com vírus e *malware*	• Ataques de usuários mal-intencionados; • Roubo de informações confidenciais; • Divulgação de informações privadas; • Perda de dados.
Ameaças Internas	• Uso indevido da rede; • Acesso à arquivos não autorizados.
Energia elétrica	• Falta de um sistema alternativo de energia; • Afeta vendas, faturamento e todas as rotinas administrativas desenvolvidas diariamente; • Longa duração das quedas de energia elétrica.
Falhas humanas	• Senhas fracas; • Falta de preparo na utilização das redes; • Alteração e remoção de arquivos indevidos; • Maquinas infectadas por vírus.
Ausência de *backup* regular	• Perda de dados parcial ou total.
Monitoramento e segurança	• Local desprotegido; • Empresas ficam vulneráveis à roubos devido à entrada sem fiscalização e controle.

Fonte: Elaborado pelo autor

3.4 Recomendações e Melhorias

Com a identificação das principais fraquezas e ameaças disposta no Ponto Brasil, foram sugeridos pelo autor as seguintes recomendações e melhorias:

3.4.1 Criação de políticas de SI

O autor sugere o uso das seguintes políticas de SI visando a melhoria da segurança das informações e dos próprios usuários:

- **Autenticação:** O *coworker* tem total responsabilidade sobre seu *login* e senha e de todos os procedimentos efetuados com seu identificador nos recursos do *coworking*. É necessário:

a) Criar senhas conforme as regras de complexidade: a senha não pode conter o nome do usuário; senha deve conter pelo menos oito caracteres; senha com letras maiúsculas, minúsculas números e caracteres especiais;
b) Memorizar as senhas e não as registrar em lugar nenhum;
c) Alterar as senhas periodicamente, no intervalo de 3 meses, sem repetição das últimas 3 utilizadas pelo usuário;
d) Não permitir o uso do *login* por outras pessoas;
e) Sempre bloquear o dispositivo ao sair da sua estação de trabalho.

- **Mesa e tela limpa:** Nunca deixar a mostra informações confidenciais, seja em dispositivos eletrônicos, em papeis ou coladas na tela do computador de forma física (*post-it*) ou eletrônica (notas digitais).
- **Informações em locais públicos:** Evitar conversas confidenciais em locais públicos ou por mensagens eletrônicas.
- **Uso de *e-mail*:** Por se tratar do meio de comunicação mais utilizado pelas empresas é necessário atenção especial aos seguintes tópicos:

a) Somente abrir anexos com as extensões *.bat, .exe,.src, .lnk* e .com se houver solicitado arquivos nesses formatos;
b) Cuidado com assuntos nomeados de forma estranha e/ou em inglês;
c) Não repasse *e-mails* do tipo corrente.

- **Política social:** Para melhoria da segurança do Ponto Brasil, sugere-se que:

a) Não fale sobre as políticas de segurança utilizadas em local externo;
b) Não repasse sua senha para ninguém;
c) Não digite sua senha e usuário em máquinas de terceiros.

- **Antivírus:** Os *coworkers* devem utilizar o *software* antivírus indicado pelo Ponto Brasil e manter as definições de vírus atualizadas constantemente.

O não cumprimento dessas políticas acarretará em sanção administrativas, podendo levar à proibição do uso do espaço, dependendo da gravidade da ocorrência.

3.4.2 Utilização de antivírus padronizado

Fundamentalmente é de grande importância entender o que é o chamado vírus. Os vírus são pequenos programas criados para ocasionar algum dano ao usuário. Essas ameaças podem vir de vários lugares *e-mails*, *websites* suspeitos, *pendrives* e até mesmo de programas baixados ilegalmente. Existem vários tipos de vírus, os mais comuns e conhecidos são os *Trojans* (Cavalo de Tróia) que são utilizados para ter acesso ao computador da vítima; *Spywares* utilizados para roubo de logins e senhas; *Malwares*, utilizado para roubar informações, divulgar serviços, apagar dados, entre outros. Quando os dispositivos corporativos são infectados, a rede pode sofrer lentidão, o que, consequentemente diminui a produtividade dos usuários e abre brecha para vazamento de informações confidenciais.

Em muitos casos os empresários não se preocupam ou não conhecem os riscos de se utilizar soluções de antivírus domésticas para proteger os dispositivos da sua empresa, e, assim, escolhem essa estratégia, por achar que estão economizando. As ferramentas de uso doméstico são pouco eficazes, pois não foram criadas para um ambiente coorporativo. Portanto, se o sistema da empresa for infectado, toda a economia poderá ser empregue para conter as ameaças.

Outra questão a se preocupar, é que usar softwares não corporativos é infringir Lei Brasileira de Software, podendo ter que responder na justiça por essa falha.

Os antivírus corporativos são projetados com o objetivo de proteger as corporações e são mais adequados para suas necessidades especificas.

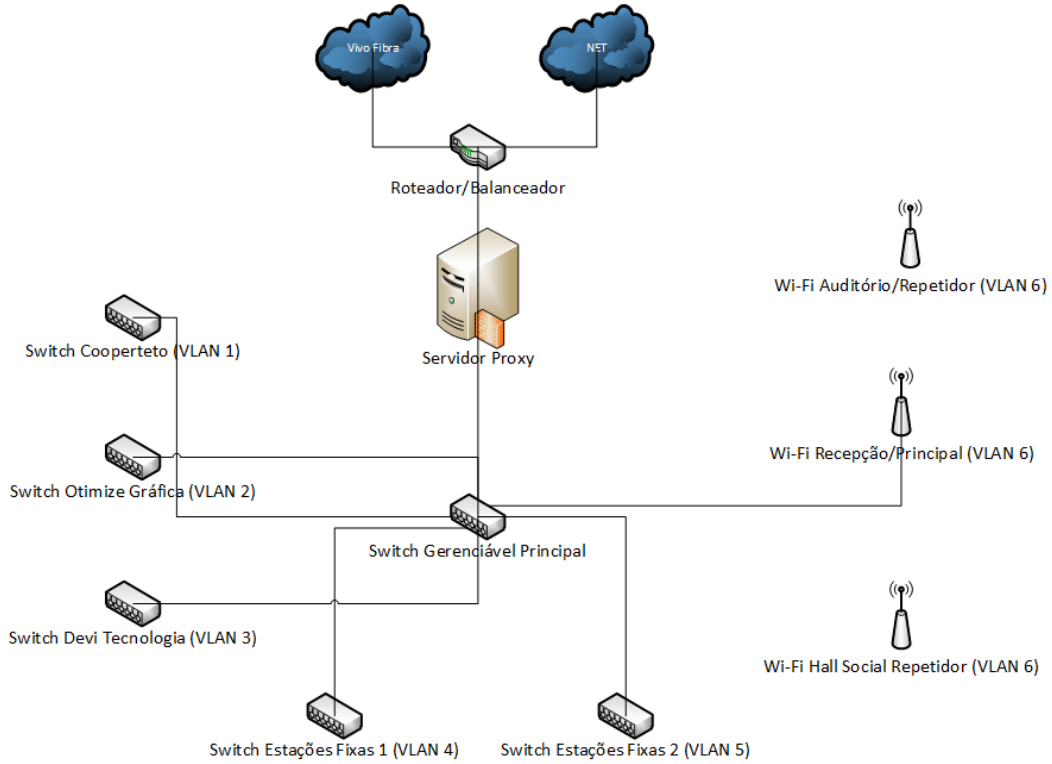
Todos os *coworkers* deverão utilizar um sistema de antivírus corporativo que será disponibilizado pelo próprio *coworking*, um valor adicional na mensalidade será agregado para suprir essa necessidade.

3.4.3 Nova configuração da infraestrutura de redes

Continuando na topologia de rede do tipo estrela, o autor sugere que adicione um servidor *proxy* para autenticação dos usuários na rede, monitoria de trafego, gerenciamento de cache e *firewall* (bloqueio de acessos para diminuir a vulnerabilidade) conectado ao roteador/balanceador. Ainda possuirá um *switch* gerenciável principal, onde será configurado redes *VLAN* (*Virtual LAN)* para cada sub-*switch* e w*i-fi* com o objetivo de dividir logicamente os acessos entre cada local e

restringir as informações. A rede *VLAN* 1 será utilizada pela empresa Cooperteto, a rede *VLAN* 2 e 3 serão utilizadas pela Otimize gráfica e Devi Tecnologia, respectivamente, e as redes *VLAN* 4 e 5 são de uso das estações fixas. As estações compartilhadas, os visitantes e os dispositivos móveis dos usuários utilizarão a rede *wi-fi* (*VLAN* 6), no qual sugere-se a instalação de dois repetidores para melhoria de sinal, um no auditório e outro no Hall Social. Os servidores existentes serão desativados com a migração dos softwares de gestão da Cooperteto e do Ponto Brasil para tecnologia em nuvem. A nova estrutura de redes está apresentada abaixo, de acordo com a Figura 5:

Figura 5: Projeto de rede sugerido para Ponto Brasil



Fonte: Elaborado pelo autor

Com a implantação dessas alterações, a rede terá controle de usuários e monitoramento dos acessos, se tornando mais eficiente, segura e mais rápida.

3.4.4 Aquisição de *nobreaks* e geradores

Os nobreaks são equipamentos indispensáveis para se evitar perdas de dados e falhas do sistema operacional, funcionando como um equipamento auxiliar quando existe queda de energia. Proporciona um tempo extra de autonomia para que tarefas sejam finalizadas ou que o computador possa ser desligado em segurança. Também tem a função de filtrar a energia fornecida para os equipamentos, evitando danos aos equipamentos conectado a ele. Serão implementados *nobreaks* nos equipamentos da rede do ponto Brasil, se estendendo o tempo de duração de sua disponibilidade.

É importante destacar que apenas os *nobreaks* não são suficientes para suprir a falta de energia de um espaço compartilhado, onde empresas dependem do uso dos equipamentos para seu funcionamento. Por esse motivo, é de suma importância a instalação de um gerador para fornecimento ininterrupto de energia. Isto é muito importante, uma vez que permite as empresas trabalharem normalmente e garantir a preservação da integridade do sistema.

3.4.5 Instalação de um sistema de segurança

Mesmo que as empresas possuam os melhores *firewalls*, antivírus e sistemas de proteção que garantam boa parte da integridade de seus dados é preciso saber que a segurança da informação vai muito além do que proteger a rede de vírus ou ameaças de roubo de informações de um banco de dados. Desta forma, as corporações devem analisar os riscos que, podem ser, desde uma restrição de acesso de uma pessoa até perdas de informações causadas por causas naturais. É de grande importância o controle e monitoramento de um escritório compartilhado, pois sempre existe uma grande movimentação que dificulta o controle de acesso se não houver um sistema eficiente de monitoramento. O sistema de câmeras além de permitir visualizar e registrar imagens de diversos ambientes age diretamente com o fator psicológico de dissuasão.

3.4.6 *Backup* do servidor *proxy* e das configurações de rede

O backup existe para evitar a perda de dados, como arquivos deletados acidentalmente por falha física ou humana, garantindo assim a integridade dos dados,

de configurações, banco de dados e arquivos de usuários. Os *backups* devem ser armazenados em locais seguros com acesso restrito apenas as pessoas com permissão de acesso aos dados, e protegido também contra os agentes nocivos da natureza, como a poeira, calor e umidade. Após a geração de um *backup* é essencial que se faça a verificação, em intervalos regulares. Isso garante que o arquivo de *backup* esteja 100% integro caso surgir a necessidade de utiliza-lo.

No Ponto Brasil, sugere-se a execução de *backups* regulares do servidor de *proxy* e dos equipamentos de rede, sempre verificando se o arquivo gerado está completo e pronto para ser restaurado. Utilizaremos o Microsoft Azure Backup para armazenamento com acesso apenas do administrador da rede.

4. CONSIDERAÇÕES FINAIS

O estudo desenvolveu uma análise do funcionamento da segurança da informação em espaços do *coworking.* Por se tratar de uma tendência em crescimento, tornou-se importante avaliar a confidencialidade, integridade e

disponibilidade da informação em ambientes de trabalho compartilhado. O local escolhido para desenvolvimento do estudo foi o Ponto Brasil, localizado em Americana, interior de São Paulo.

Complementando, foi efetuado a conceituação de *coworking* e dos princípios básicos de segurança da informação, para comparação entre ambos os sistemas com o intuito de verificar os processos de proteção dos dados.

A partir do levantamento dos dados, percebeu-se que o ambiente do Ponto Brasil era funcional, fornecendo uma estrutura adequada aos *coworkers*, entretanto havia brechas no quesito de Segurança da Informação, tais como: inexistências de políticas de SI para regulamentar e orientar os usuários; vulnerabilidade à danos com vírus e *malware* pela não adequação dos antivírus utilizados; não possuir sistema alternativo de energia elétrica em casos de queda no fornecimento; ausência de *backup* regular, inexistência de um sistema de monitoramento e segurança.

Com isso, o autor sugere que sejam feitas melhorias para aumentar a segurança e eficiência do local estudado, com estratégias como: criar políticas de SI para formalização de normas; utilização de antivírus corporativo padrão; alteração na infraestrutura de redes para maior proteção e eficácia do *coworking;* instalação de *nobreaks* e gerador de energia, além da instalação de um servidor *proxy* e sistema de câmeras.

Considera-se que os espaços de *coworking* são locais que possibilitam uma melhoria nos custos das empresas e oferece ótimas oportunidades de *networking*, porém é necessário a preocupação com as redes de informação utilizadas para garantir que seja um local seguro, além de econômico e inovador.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC. Tecnologia da Informação – **Técnicas de Segurança – Código de prática para a gestão da segurança da informação**. ISO/IEC 27001:2013.

_____. Tecnologia da Informação – **Técnicas de Segurança – Código de prática para a gestão da segurança da informação.** ISO/IEC 27002:2013.

ALLEN. D. & BERG, C. ***The sharing economy: How over-regulation could destroy an economic revolution***. Disponível em <http://ipa.org.au/publications/2312/the-sharing-economy-how-over-regulation-could-destroy-an-economic-revolution>. Acesso em 13 de março de 2017.

BEAL, A. **Segurança da Informação**: **princípios e melhores práticas para a proteção dos ativos de informação nas organizações.** São Paulo: Atlas, 2005.

CAMPUS.CO. ***Campus São Paulo*** Disponível em <https://www.campus.co/sao-paulo/pt/about>. Acesso em 25 de outubro de 2017.

CASANAS, Alex Delgado Gonçalves; MACHADO, César de Souza. **O impacto da implementação da norma NBR ISO/IEC 17799 – código de prática para a gestão da segurança da informação nas empresas.** Anais em CDROM do XXI Encontro Nacional de Engenharia de Produção, Salvador-BA, 2001.

COWORKING BRASIL. **Censo Brasil 2017**. Disponível em: <https://coworkingbrasil.org/censo/2017-estudo-completo/>. Acesso em 11 de novembro de 2017.

_____. **Como funciona o *Coworking*?** Disponível em <http://coworkingbrasil.org/como-funciona-coworking/>. Acesso em 11 de novembro de 2017.

CWBE *COWORKING*. **O que é *coworking*?** Disponível em: <http://www.cwbecoworking.com.br/2017/10/27/o-que-e-coworking/>**.** Acesso em 15 de novembro de 2017.

DAUNORIENĖ, A., DRAKŠAITĖ, A., SNIEŠKA, V., & VALODKIENĖ, G. ***Evaluating Sustainability of Sharing Economy Business Models.*** *Procedia-Social and Behavioral Sciences*, 213, 836-841; 2015.

DE OLIVEIRA, Fernando Ventura; FREITAS FILHO, Fernando Luiz; LANZER, Edgar Augusto. **Espaços de *Coworking* como Fomentadores ao Ecossistema Empreendedor: O caso brasileiro do CUBO.** Revista ESPACIOS| Vol. 37 (Nº 27) Año 2016, 2016.

DOULAMIS, T. ***Coworking. Master of arts thesis.*** *Department of Design, Virginia Commonwealth University, Richmond, USA; 2013*.

ELOCOWORKING. ***Elo Coworking*** Disponível em < http://elocoworking.com.br/>. Acesso em 25 de outubro de 2017.

_____ . ***Elo Coworking: Vantagens e facilidades.*** Disponível em <http://elocoworking.com.br/sobre>. Acesso em 25 de outubro de 2017.

GANDINI, A. ***The rise of coworking spaces: a literature review.*** *Ephemera*: theory & politics in organization, 15(1), 193-205; 2015.

IMPACT HUB. ***Impact Hub.*** Disponível em <http://saopaulo.impacthub.com.br/>. Acesso em 25 de outubro de 2017.

KONZEN, Marcos Paulo et al. **Gestão de Riscos de Segurança da Informação Baseada na Norma NBR ISO/IEC 27005 Usando Padrões de Segurança**. 2013.

LEFORESTIER, Anne. ***The coworking space concept.*** *2009, 19p. CINE Term Project. Indian Institute of Management (IIMAHD). Ahmedabad.*

MUNHOZ, A. et al. ***Coworking* e *crowdsourcing*: como modelos de negócios inovadores influenciam no desenvolvimento de *start-ups*.** Anais do XVI Semead–Seminários em Administração. São Paulo, SP, Brasil, 2013.

MARCIANO, João Luiz Pereira; LIMA-MARQUES, Mamede. O **enfoque social da segurança da informação.** 2006.

_____. **Segurança da informação: uma abordagem social.** 2009.

O ESTADAO. Google **inaugura espaço voltado para empreendedores em São Paulo**. Disponível em <http://link.estadao.com.br/noticias/inovacao,google-inaugura-espaco-voltado-para-empreendedores-em-sao-paulo,10000055716>. Acesso em 25 de outubro de 2017.

OWYANG, Jeremiah; TRAN, Christine; SILVA, Chris. ***The collaborative economy.*** *Altimeter, United States*, 2013.

RAMOS, A. **Guia Oficial para Formação de Gestores em Segurança da Infomação: *Secutity Officer 1*.** Zouk: Porto Alegre, 2008.

SACHS, I. **Inclusão Social pelo Trabalho – Desenvolvimento Humano, Trabalho Decente e o Futuro dos Empreendedores de Pequeno Porte**. Rio de Janeiro: Garamond, 2003.

SCUDERE, Leonardo. **Risco digital**. Elsevier Brasil, 2006.

SEBRAE. **Como as incubadoras de empresas podem ajudar o seu negócio** Disponível em <https://www.sebrae.com.br/sites/PortalSebrae/artigos/as-incubadoras-de-empresas-podem-ajudar-no-seu-negocio,f240ebb38b5f2410VgnVCM100000b272010aRCRD>. Acesso em 25 de outubro 2017.

SFREDDO, J. A.; FLORES, D. **Segurança da informação arquivística: o controle de acesso em arquivos públicos estaduais. Perspectivas em Ciência da Informação**, v. 17, n. 2, p. 158-178, 2012. Disponível em: <http://basessibi.c3sl.ufpr.br/brapci/v/a/12726>. Acesso em: 02 de outubro de 2017.

SILVA NETTO, Abner da; PINHEIRO DA SILVEIRA, Marco Antonio. **Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas**. ***JISTEM: Journal of Information Systems and Technology Management****,* v. 4, n. 3, 2007.

SOARES, Juliana Maria Moreira; SALTORATO, Patricia. ***Coworking,* uma forma de organização de trabalho: conceitos e práticas na cidade de São Paulo.** AtoZ: novas práticas em informação e conhecimento, v. 4, n. 2, p. 61-73, 2015.

SPINUZZI, C. *Working alone together coworking as emergent collaborative activity.* ***Journal of Business and Technical Communication***, 26(4), 399-441; 2012.

TIPTON, H. F. ***Types of Information Security Controls****. Information Security Management Handbook.* 5 ed. Boca Raton, CRC Press, 2004. p 113-125

TITTEL, E. CHAPPLE, M. STEWART, J. M.CISSP®: ***Certified Information Systems Security Professional - Study Guide****.* Sybex: San Francisco, 2003.

TURBAN, Efraim et al. **Tecnologia da Informação para Gestão-: Transformando os Negócios na Economia Digital**. Bookman, 2010.

ZAGO, Graziella Dora. **Conexão de espaços e ideias: incubadora no cruzamento.** Farrapos-Ramiro. 2016.