FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

Gabriel Fernando Pereira dos Santos
Matheus Pestana Amorim

Segurança da Informação em escritórios contábeis: Um estudo de caso

Americana, SP

2019

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Gabriel Fernando Pereira dos Santos

Matheus Pestana Amorim

Segurança da Informação em escritórios contábeis: Um estudo de caso

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do (a) Prof.(a) especialista Marcurs Vinícius Lahr Giraldi.

Área de concentração: Segurança da informação

Americana, SP.

2019

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

S235s SANTOS, Gabriel Fernando Pereira

Segurança da Informação em escritórios contábeis: um estudo de caso. / Gabriel Fernando Pereira Santos, Matheus Pestana Amorim. – Americana, 2019.

51f.

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

Orientador: Prof. Esp. Marcurs Vinícius Lahr Giraldi

1 Segurança em sistemas de informação I. AMORIM, Matheus Pestana II. GIRALDI, Marcurs Vinícius Lahr III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: *681.518.5*

Gabriel Fernando Pereira dos Santos
Matheus Pestana Amorim

Segurança da informação em escritórios contábeis: Um estudo de caso

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 junho de 2019.

Banca Examinadora:

Marcus Vinícius Lahr Giraldi(Presidente)
Especialista
Fatec Americana

Renato Kraide Soffner (Membro)
Doutor
Fatec Americana

Renan Mercuri Pinto (Membro)
Doutor
Fatec Americana

AGRADECIMENTOS

Em primeiro lugar gostaríamos de agradecer a Deus, por ter nos dado força para a conclusão deste trabalho, agradecemos aos nossos familiares, amigos, que nos acompanharam nesta trajetória, nos encorajando e dando força e incentivo até esta conclusão.

Por fim agradecemos ao nosso professor orientador Marcus Lahr, pelas horas disponibilizadas, pelas dicas, orientações e correções, onde foi possível chegarmos a este resultado.

DEDICATÓRIA

Aos nossos familiares, especialmente pais e sogros, amigos mais próximos e a Deus.

RESUMO

O presente texto conceitua e define o ambiente contábil e as informações que transitam dentro dele, mostrando a importância e o grande impacto que a informática tem nas interações da contabilidade com todos seus clientes. Sobretudo demonstrando os principais riscos e problemas que o setor pode enfrentar com uma situação que explore as suas vulnerabilidades de segurança digital ou dos ativos *offline* como documentos e arquivos, sugerindo então uma melhoria voltada aos pilares da segurança da informação com controles de *frameworks* de cibersegurança. Através de um estudo de caso este trabalho demonstra com cálculos e resultados o grau de risco que os ativos informatizados estão expostos e propõem melhorias que causam resultados consideráveis no cotidiano do setor contábil. Não levando em conta o valor de investimento e manutenção, mas contextualizando a necessidade da segurança da informação e da informática nos ambientes contábeis.

Palavras Chave: Segurança da informação, Segurança contábil, Segurança digital

ABSTRACT

The present text conceptualizes and defines the accounting environment and the information that transits within it, showing the importance and the great impact that computer technology has on accounting interactions with all its clients. Above all, it demonstrates the major risks and problems the industry can face with a situation that exploits its digital security vulnerabilities or offline assets such as documents and files, suggesting an improvement in the cornerstones of information security with controls of cybersecurity frameworks. Through a case study this work demonstrates with calculations and results the degree of risk that the computerized assets are exposed and propose improvements that cause considerable results in the daily life of the accounting sector. Not taking into account the value of investment and maintenance, but contextualizing the need for information and information security in accounting environments.

Palavras Chave: *Security Information, Accounting, Digital Security*

SUMÁRIO

Sumário

1 INTRODUÇÃO 11

2 CONTEXTUALIZAÇÃO DE UM ESCRITÓRIO CONTÁBIL 12

2.1 DADOS QUE TRANSITAM NA CONTABILIDADE 13

2.2 O AVANÇO DA TECNOLOGIA CONTÁBIL 16

3 RISCOS E VULNERABILIDADES EM UM ESCRITÓRIO CONTABIL 18

3.1 RISCOS 18

3.2 VULNERABILIDADES 18

3.3 SEGURANÇA DA INFORMAÇÃO 19

3.4 SEGURANÇA DA INFORMAÇÃO E O AMBIENTE CONTÁBIL 21

4 ESTUDO DE CASO 22

4.1 LEVANTAMENTO DE ATIVOS 22

4.1.1 Ativos de TI ---------- 22

4.1.2 Ativos Offline ---------- 24

4.2 LEVANTAMENTO DE AMEAÇAS PARA O NEGÓCIO 25

4.3 ANÁLISE QUANTITATIVA DOS RISCOS 35

4.4 LEVANTAMENTO DA PRIORIZAÇÃO DOS RISCOS 39

5 PROPOSTA DE MELHORIA 41

5.1 IMPLEMENTAÇÃO DE CONTROLE DE MOVIMENTAÇÃO DE DOCUMENTOS 41

5.2 MEDIDAS DE CONTINUIDADE 42

5.3 MEDIDAS DE CONTROLE DE ACESSO: 42

5.4 SEGURANÇA A USUÁRIOS: 43

5.5 MEDIDAS DE SEGURANÇA OU DE DISPOSIÇÃO FÍSICA DOS ATIVOS: 44

5.6 RESULTADO DAS MELHORIAS 44

6 CONSIDERAÇÕES FINAIS 48

LISTA DE FIGURAS

Figura 1 -Pilares da Segurança da Informação.....21
Figura 2 - Valor de risco antes da implementação da proposta de melhoria.....46
Figura 3 Comparação entre os valores de risco antes e depois da proposta de melhoria 47

LISTA DE TABELAS

Tabela 1 - Ativos Térreo.....23
Tabela 2 - Ativos Primeiro Andar 23
Tabela 3 - Ativos Segundo Andar 23
Tabela 4 - Ativos Terceiro Andar 24
Tabela 5 - Ativos Offline.....25
Tabela 6 - Vulnerabilidades Ativos Térreo 25
Tabela 7 - Vulnerabilidades Ativos Primeiro Andar 26
Tabela 8 - Vulnerabilidades Ativos Segundo Andar.....28
Tabela 9 - Vulnerabilidades Ativos Terceiro Andar.....30
Tabela 10 - Vulnerabilidades Ativos *Offline* 33
Tabela 11 Análise Quantitativa Ativos Térreo.....37
Tabela 12 Análise Quantitativa Ativos Primeiro Andar.....37
Tabela 13 Análise Quantitativa Ativos Segundo Andar 37
Tabela 14 Análise Quantitativa Ativos Terceiro Andar 38
Tabela 15 Análise Quantitativa Ativos *Offline* 39
Tabela 16 Ativos com maior índice de risco.....39
Tabela 17 - Análise Quantitativa após a Implementação da Proposta 44
Tabela 18 - Redução em (%) em cada Ativo.....45

1 INTRODUÇÃO

Segurança da informação é um assunto bastante abordado na atualidade, pois em um mundo tão informatizado e conectado fica difícil não encontrar algum setor da economia que não seja influenciado pela evolução da tecnologia, independentemente de impactar na produtividade ou na qualidade de um produto ou serviço.

Tal tecnologia influencia também a comunidade contábil, que através de novos recursos lançados todos os dias, busca aperfeiçoar e ampliar suas linhas de atendimento e qualidade. Com esta atual necessidade, revela-se um questionamento sobre quais são as principais vulnerabilidades que podem ser encontradas nos dados e informações que transitam entre contador e as empresas, diante de uma má gestão e uma má implantação dos ativos e sistemas.

Os dados que são gerenciados por um escritório contábil, constituem toda a essência de uma empresa, compondo informações com elementos de dados de funcionários, informações bancárias, e toda movimentação regularizada de um empreendimento, sendo que com um mau gerenciamento destes dados, podem haver prejuízos tanto para o escritório, quanto para a empresa.

Por conta disto, um estudo da segurança em ambientes contábeis torna-se relevante, pois é uma área que tem acesso a todos os tipos de dados das empresas e em muitos cenários estão indevidamente protegidas das ameaças existentes do cotidiano, como acessos indevidos a dados confidenciais, perda de dados e documentações.

2 CONTEXTUALIZAÇÃO DE UM ESCRITÓRIO CONTÁBIL

Para entender qual é o grau de importância da Segurança da Informação dentro de um escritório contábil, é necessário analisar, o que compõe um escritório contábil e a partir disso desenvolver a imagem do escritório, que geralmente é representada por muitos como um ambiente cheio de documentos e papéis e de muita pessoas calculando impostos e mais impostos.

A Contabilidade está presente na história humana desde os primórdios dos tempos. Estudos afirmam que ela teve início desde os tempos da pré-história com registros de produções agrícolas e de criação de animais, onde ao passar do tempo com o desenvolver da humanidade, foi se criando uma necessidade de estabelecer registros apurados com informações relevantes. Segundo MILLS (1994)

> "[...] "Livros contábeis foram abertos e no início do século XIV os primeiros manuscritos revelaram débitos e créditos em parágrafos verticalmente dispostos. Isto era uma evidência de que razões com sistema de partidas dobradas existiam desde 1335[...]"

A Contabilidade evoluindo juntamente à sociedade passou a ser um instrumento eficaz, capaz de auxiliar na administração de um empreendimento fornecendo informações sensíveis capazes de influenciar o processo decisório e analítico das empresas, como dito por Lucas (2009), em seu trabalho de iniciação científica:

> "[...] Devido ao progresso causado pela globalização, e as novas oportunidades que surgem através do avanço na área tecnológica. O contador se torna um fornecedor de informações contábeis e financeiras para as organizações, nas suas decisões. O contador deve ser visto pela sociedade e por seus clientes, como um gerador de informações. Informações essas que se tornam essências e diferenciais [...]"

Contabilidade é definida por um trabalho minucioso com procedimentos e análises fiscais, trabalhistas e tributárias como explicado no portal da contabilidade (2006), onde é possível ter uma explicação breve do que é e o que faz um escritório:

> “[...]Contabilidade é um trabalho minucioso de análise das áreas fiscal, tributária e trabalhista de uma empresa, instituição ou entidade governamental ou não governamental. Portanto, é uma atividade que exige tempo para análise.
> Muitas empresas contratam firmas ou escritórios de contabilidade para prestar esse serviço. Em muitos casos, não há vantagem financeira em manter uma estrutura contábil. Até mesmo porque muitas empresas são obrigadas a realizar auditorias periódicas.
> Por essas razões, em alguns casos, é vantagem a empresa contratar um escritório de contabilidade, que passa a ser responsável pelo balanço contábil e financeiro, pagamento de tributos, resoluções de problemas relativos ao quadro de funcionários, entre outras questões relativas à contabilidade empresarial[...]”

Analisando a citação acima é possível ter o entendimento que um escritório contábil possui dentro de seus serviços diversas atividades que atendem a diversos âmbitos como a área fiscal ou, por exemplo, a trabalhista. Ou seja, é um ambiente que trabalha com análise minuciosa de diversas informações dos mais variados setores de uma determinada empresa, podendo esse escritório contábil ser interno, em outras palavras ser dentro de uma determinada empresa, ou então externo, como um serviço terceirizado a um escritório contábil.

2.1 DADOS QUE TRANSITAM NA CONTABILIDADE

A contabilidade possui um extenso portfólio de obrigações periódicas, que são resultantes a partir do processamento de muitos dados, onde com analises e auditorias nos âmbitos fiscais, contábeis, trabalhistas e societário se geram guias de impostos e obrigações acessórias, que são obrigatoriamente entregues ao governo Brasileiro e repassadas aos clientes da contabilidade, como é possível ver na página Osayk (2019) onde é apresentado o que são as obrigações contábeis, não somente as guias de impostos, a contabilidade é muito mais do que isso:

> “[...]As obrigações contábeis, fiscais e previdenciárias que as empresas precisam cumprir no Brasil não se resumem ao recolhimento de tributos.

> Além da alta carga tributária, os empresários precisam se responsabilizar por uma série de “deveres” para manter-se em situação regular e evitar colocar em risco os negócios. São declarações, regulamentações e rotinas que devem observadas.[...]”

A Contabilidade possui a responsabilidade de realizar a entrega de várias obrigações, dentro do portal de contabilidade e da página do SEBRAE é possível ter uma listagem das obrigações acessórias como por exemplo: ECF, CAGED, PIS, COFINS, ICMS entre outras obrigatoriedades, dentre elas as declarações digitais que compõem toda a movimentação oficial de uma empresa, elas são denominadas como declarações do SPED (Sistema Público de Escrituração Digital)

Os SPED’s são arquivos digitais que são entregues através dos portais e aplicativos da receita federal brasileira. Essas declarações são conhecidas por atuar em uma modernização do governo na metodologia de conseguir as informações e apurações dos resultados das empresas com uma estrutura perfeitamente auditáveis e robusta, podemos ver dentro da página do sítio SPED o que realmente são essas obrigações acessórias.

> “[...]De modo geral, consiste na modernização da sistemática atual do cumprimento das obrigações acessórias, transmitidas pelos contribuintes às administrações tributárias e aos órgãos fiscalizadores, utilizando-se da certificação digital para fins de assinatura dos documentos eletrônicos, garantindo assim a validade jurídica dos mesmos apenas na sua forma digital. [...]”

Para o governo brasileiro os SPED’s trouxeram uma série de benefícios, possibilitando aos auditores correlacionar informações entre os arquivos digitais o que possibilita melhor controle e monitoramento nos pagamentos dos impostos brasileiros diminuindo as taxas de fraudes e outras situações, uma vez que com os arquivos toda a movimentação da empresa é relatada e pode ser auditada com facilidade devido às estruturas do arquivos e as plataformas as quais o governo tem acesso. Dentro do site do sítio SPED é possível ver quais são seus principais benefícios (acessando http://sped.rfb.gov.br/), como por exemplo a redução de custos com a dispensa de emissão e armazenamento de documentos em papel, ou

a rapidez no acesso às informações, aumentando a produtividade dos auditores com uma coleta rápida e o correlacionamento das informações entre os arquivos.

Além de uma série de benefícios aos fisco, as obrigações compostas pelos sistemas SPED's são elaboradas pelo fornecimento e escrituração de todo tipo de informação que transita na contabilidade, apresentando variações dos tipos de dados utilizados em cada declaração, contudo em uma visão geral os sistemas SPED's são compostos de informações como valores das vendas, salário de funcionários, contas e boletos pagos e recebidos, até os documentos e dados pessoais dos colaboradores, como CPF, estado civil, se possuem dependentes, entre diversas outras coisas. Essas informações são exigidas nas obrigações e apresentadas na forma de arquivos textos.

Minuciando as estruturas de todos os arquivos SPED's pode-se obter informações sensíveis das empresas. Por exemplo, o Escrituração Fiscal Digital das Contribuições (EFD Contribuições ou SPED Contribuições) trata-se de um arquivo digital com a escrituração de documentos que resultam na apuração do PIS/Pasep e da COFINS, ambos impostos que são calculados com base na tributação item a item. Ou seja, para fazer essa obrigação o contador deve ter toda a movimentação de compra e de venda de produtos, de serviços tomados e prestados, e dos transportes realizados nas transações de mercadorias.

Outro exemplo de informações sensíveis é o conteúdo da Escrituração Contábil Digital (SPED ECD) onde se abrange toda a movimentação contábil da empresa, em outras palavras cada pagamento e cada recebimento da empresa, toda a movimentação bancária e financeira da empresa.

Essas informações nas mãos certas e após processadas podem sem dúvidas compor tomadas de decisões importantes para o futuro de um empreendimento. Contudo, quando se olha por outro lado, a mesma informação nas mãos erradas pode ser utilizada como arma. No meio das informações citadas existem aspectos como os preços negociados com fornecedores e com clientes, além de questões como os salários e benefícios negociados com os colaboradores, abrangendo a carga horária e localização dos mesmos, além da existência de informações da saúde financeira da empresa, quem ela paga e de quem ela recebe. Em uma situação hipotética se essas informações caíssem nas mãos de um concorrente ele conseguiria estruturar estratégias que fossem melhores e realizar negociações com

clientes e fornecedores com dados vitais como forma de pagamento e preços melhores.

2.2 O AVANÇO DA TECNOLOGIA CONTÁBIL

A Contabilidade se estabelece como uma prestação de serviço na qual se trabalha muitas informações. A grande questão é que para trabalhar e atender a alta demanda fiscal e a exorbitante quantidade de informações, a contabilidade precisa de recursos tecnológicos para sintetizar processos e escalar suas demandas com seus clientes.

A tecnologia estabelece sobretudo conexão entre os serviços, colaboradores, clientes e o governo, conexão que explora recursos da informática que estão cada vez mais integrados, como cita a empresa Wolters Kluwer (2017) fornecedora de softwares para empresas contábeis.

> “[...]O mercado contábil sofreu, como poucos, um impacto enorme pela digitalização e expansão da Internet nos últimos anos. Não bastasse a adoção em larga escala da conectividade pelas pessoas físicas e jurídicas, os órgãos fiscalizadores e arrecadadores do país estão cada vez mais integrados aos sistemas de bancos, cartórios, prestadores de serviço entre outros. [...]”

Quando se avalia a situação contábil no Brasil hoje em dia, é possível ver a grande expansão tecnológica, onde se presencia a evolução do setor, onde o mesmo saiu da escrituração de documentos e papéis para arquivos digitais e informações integradas como os SPED. Diante desse cenário estabelece uma noção da evolução pelo qual o setor tem passado e mostrando os cenários pelo quais ainda vai evoluir, de acordo com Marcelo Lombardo fundador da empresa OMIE (2015), software digital, para empresários e contadores diz que questões como a tecnologia e a inovação de serviços definirão o futuro do setor,

> “[...]Baseado no "Merger Endgame" do At Kearney, pontuo como os fatores de complexidade, tecnologia, automação, crescimento, preços, concorrência e comportamento, estão relacionados ao crescimento e o futuro da contabilidade. [...]”

Concluindo que a Evolução tecnológica para o setor se encontra em evolução e crescente desenvolvimento destaca-se que ainda existe a demanda de inovação e necessidade de adaptações e automações tecnológicas no setor.

Diante de tudo isso, fica claro que muitos desafios ainda precisam ser superados pela contabilidade: desde a necessidade de incorporação das novas tecnologias pelas empresas contábeis, até a compreensão dos efeitos dessas tecnologias. Será cada vez mais exigido do setor, conhecimentos e tecnologias que proporcionem automações e verificações, em processos contínuos, tornando-se cada vez mais necessária a existência de fatores tecnológicos para isso.

3 RISCOS E VULNERABILIDADES EM UM ESCRITÓRIO CONTABIL

Conforme abordado no capítulo 2, é possível perceber que a contabilidade tem acesso a diferentes tipos de informações, sendo ela fiscal, trabalhista ou financeira. Com posse de todos estes dados, a Contabilidade possui a habilidade de conhecer a real situação da empresa, apontando características que talvez não estejam englobados à visão do empreendedor.

3.1 RISCOS

Para que seja melhor o entendimento, dos problemas que um escritório possui, quanto a segurança da informação, é necessário compreender a definição de risco. Segundo Bezerra, (2013), em seu estudo sobre a norma NBR 27005, a definição de risco consiste em:

> "[...]Risco: combinação da probabilidade (chance da ameaça se concretizar) de um evento indesejado ocorrer e de suas consequências para a organização. É a incerteza resultante da combinação da probabilidade de ocorrência de um evento e suas consequências.[...]"

Através desta definição, é possível compreender que o risco é um conjunto de fatores, também é possível dimensionar o grau de seu problema. Conforme a norma NBR 27005, possui cálculos para qualificar o tamanho do risco.

3.2 VULNERABILIDADES

Para melhor compreensão, para os capítulos seguintes, também é necessária a compreensão de Vulnerabilidades. Segundo Bezerra, (2013), em seu estudo sobre a norma NBR 27005, Vulnerabilidade define-se como:

> "[...]Vulnerabilidade é qualquer fraqueza que possa ser explorada para comprometer a segurança de sistemas ou informações. Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.[...]"

Quando é abordado o assunto de Vulnerabilidade, é importante também compreender a diferença entre Vulnerabilidade e Ameaça. Conforme a definição de ameaça no dicionário: Sinal, manifestação que leva a acreditar na possibilidade de ocorrer alguma coisa, Já a definição de Vulnerabilidade conforme o mesmo dicionário seria: Característica, particularidade ou estado que é vulnerável; qualidade que pode se encontrar vulnerável: a vulnerabilidade da segurança pública.

Os dois termos possuem definições muito parecidas, e que leva a confusão entre os dois. Segundo Bezerra, (2013), em seu estudo sobre a norma NBR 27005, a diferença entre Vulnerabilidade e Ameaça, define-se como:

> "[...]Entende-se que a ameaça é o evento ou incidente, enquanto a vulnerabilidade é a fragilidade que será explorada para que a ameaça se torne concreta. Ameaças podem assumir diversas formas, como furto de equipamentos, mídia e documentos, escuta não autorizada, incêndio, inundação e radiação eletromagnética, até fenômenos climáticos e sísmicos. Por exemplo, um computador cuja senha seja do conhecimento de todos, sofre ameaças como roubo, destruição ou alteração de informações; a vulnerabilidade que permite que estas ameaças se concretizem é justamente a senha ser conhecida e compartilhada por todos.[...]"

3.3 SEGURANÇA DA INFORMAÇÃO

Quando é levantado o assunto de riscos e vulnerabilidades, também é necessário abordar um tema que está correlacionado com estes assuntos: Segurança da Informação. Um tema que tem recebido mais atenção conforme o avanço da tecnologia, e a necessidade cada vez maior de produzir mais agilidade, precisa e de uma forma segura, tem contribuído para esta área da tecnologia.

Conforme abordado nos capítulos anteriores, é possível compreender como o escritório contábil trata diversos tipos de informações, e muitas destas informações são confidenciais, que não deve ser manipulados, ou obtidos por pessoas não autorizadas. Com toda esta informação, torna-se muito importante o uso e compreensão da Segurança Informação em um ambiente contábil. Conforme a definição de Sêmola (2014), a definição de Segurança da Informação seria:

> “[...]Podemos definir segurança da informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. De forma mais ampla, podemos também considerá-la como a prática de gestão de riscos incidentes que impliquem o comprometimento dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação.[...]”

Com esta definição, é possível compreender que segurança da informação, é uma área muito importante, não apenas para o ambiente contábil, mas também para outros ambientes de negócio.

A segurança da informação, é um assunto composto por pilares, sendo que se não houver um destes pilares, não será possível considerar que um ambiente seja considerado seguro. Estes pilares são conhecidos como a siglas CID, sendo eles Confidencialidade, Integridade e Disponibilidade. Conforme a definição de Sêmola (2014), estes pilares possuem a seguinte definição:

> “[...]A segurança da informação tem como objetivo a preservação de três princípios básicos que norteiam a implementação dessa prática.
> Confidencialidade — Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas a quem é destinada.
> Integridade — Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais.
> Disponibilidade — Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que eles necessitem delas para qualquer finalidade.[...]”

Uma forma de contextualizar a segurança de informação, seria através de um tripé, onde confidencialidade, integridade e disponibilidade seriam as pernas e Segurança da Informação estariam apoiadas sobre estes pilares. Retirando qualquer uma destas pernas, não será possível a estrutura se manter, como apresentado na Figura 1.

Figura 1 -Pilares da Segurança da Informação

Fonte: Ribeiro (2018)

3.4 SEGURANÇA DA INFORMAÇÃO E O AMBIENTE CONTÁBIL

Com todas essas informações sensíveis que o Escritório Contábil trata, que podem, sem dúvidas, compor tomadas de decisões importantes para o futuro de um empreendimento podem também seguindo na possibilidade de serem obtidas por usuários não autorizados, causar prejuízos enormes aos empreendimentos.

Dentro das informações citadas existem vários aspectos comerciais e gerenciais como preços, folha de pagamento, transações bancárias etc. que podem ser usadas para tirar proveito. Neste contexto, a Segurança da informação se torna cada vez mais necessária neste ambiente.

Compor um ambiente com tecnologias que proporcionem segurança e produtividade a todos os processos contábeis é um desafio que faz parte do dia a dia do setor. Sendo preciso sempre atenuar-se as novas tecnologias e sobretudo as novas ameaças para que possa sempre pensar na relação custo benéfico da informação. Pensando em compor um cenário com uma avaliação de segurança com padrões aceitáveis, foi aplicado um estudo de caso em um ambiente contábil para analisar os ativos, seus riscos, vulnerabilidades, e sobretudo o impacto que essas informações têm no cotidiano empresarial.

4 ESTUDO DE CASO

Com todo este levantamento teórico, e contextualização das obrigatoriedades e rotinas de um escritório contábil, neste capítulo será abordado os riscos e vulnerabilidades que um escritório pode sofrer em suas rotinas diárias.

Para este levantamento, foi utilizado como exemplo um escritório contábil da região metropolitana de Campinas. Este escritório atende todas as rotinas contábeis citadas nos capítulos anteriores, e este levantamento tem como objetivo apresentar as vulnerabilidades e riscos que este escritório possui. Ele também servirá de exemplo para outros ambientes contábeis, que possam estar sobre as mesmas situações.

O ambiente escolhido para este levantamento, está situado em um prédio com um Térreo, mais 3 andares, atualmente o escritório conta com um corpo de funcionário composto por 35 pessoas, sendo separados pelos setores: Contábil, Fiscal, Departamento Pessoal, Recepção e TI.

O parque computacional, conta com 3 impressoras, 1 DVR, 2 Roteadores, 5 *Notebooks*, 27 *Desktops*, 3 Servidores, 4 *Switches*, 1 Relógio Ponto, e uma Central de Alarme.

4.1 LEVANTAMENTO DE ATIVOS

Conforme descritos nos capítulos anteriores, a contabilidade trabalha com diversos tipos de informações, sendo elas também consideradas como ativos do negócio. Para melhor abordagem nesta análise, serão analisados os Ativos de TI e também os Ativos Offline, que consiste em documentações, arquivos que são manipulados pelo escritório.

4.1.1 Ativos de TI

O levantamento de ativos de TI foi realizado por andares, apontando todas as descrições e funções de cada ativo. As tabelas a seguir (tabelas de 1 a 4) contêm a descrição dos ativos de TI de cada um dos andares.

Tabela 1 - Ativos Térreo

Ativo	Descrição
Stand Alone DVR	Hospeda as câmeras, salva as gravações das câmeras
Roteador	Fornece conexão *WI-FI* para visitantes.
2 *Notebook*	Notebook da Recepção /Sala de reunião

Fonte: Próprio Autor

Tabela 2 - Ativos Primeiro Andar

Ativo	Descrição
Switch	Fornece Conexão entre os Servidores e Aplicações
Nobreak	Fornece Energia extra ao Switch em caso de queda de Energia
8 *Desktops*	Máquinas de trabalho de usuários
1 *Notebook*	Máquina de trabalho de usuário
Impressora	Fornece serviço de impressão para os usuários do Primeiro Andar

Fonte: Próprio Autor

Tabela 3 - Ativos Segundo Andar

Ativo	Descrição
Switch	Fornece Conexão entre os Servidores e Aplicações
Nobreak	Fornece Energia extra ao Switch em caso de queda de Energia
Relógio Ponto	Realiza os registros de entrada e saída dos funcionários
Impressora	Fornece serviço de impressão para os usuários do Primeiro Andar
10 *Desktops*	Máquinas de trabalho de usuários

Fonte: Próprio Autor

Tabela 4 - Ativos Terceiro Andar

Ativo	Descrição
Servidor de *Backup*	Realiza o Armazenamento dos Backup do escritório
Servidor de *Internet*	Firewall
Host VM	Hospeda uma Máquina Virtual, com o Serviço de Active *Directory*, E o serviço de Banco de dados do sistema de gerenciamento contábil
Nobreak 1	Fornece Energia extra aos Servidores em caso de queda de Energia
Nobreak 2	Fornece Energia extra aos Servidores em caso de queda de Energia
Switch	Fornece Conexão entre os Servidores e Aplicações
Repetidor	Replica o sinal *wi-fii* fornecido pelo roteador do primeiro andar
Nobreak	Proteger contra oscilação de energia
Central de Alarme	Gerencia o Alarme de todo o prédio. O mesmo está integrado na rede na empresa
Roteador *wi-fi* interno	*Wi-fi* interno sem acesso aos visitantes.
9 *Desktops*	Máquinas de trabalho de usuários
2 *notebooks*	Máquinas de trabalho de usuários
Impressora	Fornece serviço de impressão para os usuários do Primeiro Andar
Link de Comunicação	Link de *Internet*. Fornece conexão externa ao Escritório

Fonte: Próprio Autor

4.1.2 Ativos Offline

Os ativos *offline* foram classificados por setores do escritório, sendo classificados como Documentos Contábeis, Documentos Fiscais, Documentos Trabalhistas e Documentos Societários. A seguir na Tabela 5, são apresentados os ativos *offline.*

Tabela 5 - Ativos *Offline*

Ativo	Descrição
Documentos Contábeis	Boletos, Recibos de pagamentos e recebimento, extratos etc.
Documentos Fiscais	Notas fiscais, comprovantes de faturamento, guia de impostos etc.
Documentos Trabalhistas	RG,CPF,Fotos, livro registro, crachás etc.
Documentos Societários	Contratos sociais, documentos de legalização e permissão corporativas.

Fonte: Próprio Autor

4.2 LEVANTAMENTO DE AMEAÇAS PARA O NEGÓCIO

Após o levantamento de ativos se faz necessário realizar o levantamento de ameaças e vulnerabilidades, esse estudo também foi segmentado e classificado por andar. As descrições das vulnerabilidades demonstradas abaixo nas tabelas de 6 a 10, foram feitas conforme norma ABNT ISO/IEC 27005:2011..

Tabela 6 - Vulnerabilidades Ativos Térreo

Ativo	Vulnerabilidades	Ameaças	Risco
DVR	Fornecimento de Energia Instável	Interrupção do Serviço de Energia	Não será gravada as imagens de câmeras do prédio
DVR	Inexistência de mecanismos estabelecidos para o monitoramento de violações de segurança	Furto de mídia ou documentos	Perda de imagens com conteúdo sensível de procedimentos e usuários

Ativo	Vulnerabilidades	Ameaças	Risco
Roteador	Falta de uma Rotina de Substituição Periódica	Destruição de equipamento ou mídia	Clientes não poderão conectar-se a rede *wi-fi*
Roteador	Fornecimento de Energia Instável	Interrupção do Serviço de Energia	Clientes não poderão conectar-se a rede *wi-fi*
Notebooks	Atribuição errônea de direitos de acesso	Abuso de direitos	Todos os usuários possuem Permissão de administrador
Notebooks	Treinamentos insuficientes em segurança da informação	Erro durante o uso	Recepção ficará sem o ativo de TI

Fonte: Próprio Autor

Os ativos dispostos no térreo apresentados na tabela 6 compreendem uma pequena extensão dos ativos em um ambiente contábil, suas vulnerabilidades e ameaças estão diretamente relacionadas com o tipo de atividade realizada no andar, onde basicamente ocorrem a movimentação de colaboradores, clientes e terceiros.

Tabela 7 - Vulnerabilidades Ativos Primeiro Andar

Ativo	Vulnerabilidades	Ameaças	Risco
Switch	Uso inadequado ou sem os cuidados necessários de controle do acesso físico a prédios e salas	Destruição de equipamento ou mídia	O primeiro andar perderá a comunicação com a rede
Switch	Falta de uma rotina de substituição periódica	Destruição de equipamento ou mídia	O primeiro andar perderá a comunicação com a rede

Ativo	Vulnerabilidades	Ameaças	Risco
Nobreak	Sensibilidade à umidade, poeira, sujeira	Poeira, corrosão, congelamento	Em caso de queda de Energia, O primeiro andar perderá a comunicação com a rede
Nobreak	Falta de uma rotina de substituição periódica	Destruição de equipamento ou mídia	Em caso de queda de Energia, O primeiro andar perderá a comunicação com a rede
Desktops	Não execução do logout ao se deixar uma estação de trabalho desassistida	Abuso de direitos	Acesso não autorizado
Desktops	Atribuição errônea de direitos de acesso	Abuso de direitos	Todos os usuários possuem Permissão de administrador
Desktops	Fornecimento de Energia Instável	Interrupção do Serviço de Energia	Todas as máquinas estão indisponíveis
Desktops	Localização em área suscetível a inundações	Inundação	Máquinas Danificadas por inundação
Notebook	Atribuição errônea de direitos de acesso	Abuso de direitos	Todos os usuários possuem Permissão de administrador
Impressora	Fornecimento de Energia Instável	Interrupção do Serviço de Energia	Máquinas do primeiro andar não poderão realizar impressão
Impressora	Sensibilidade à umidade, poeira, sujeira	Poeira, corrosão, congelamento	indisponibilidade ou quebra do equipamento

Fonte: Próprio Autor

O primeiro andar possuí um grande conjunto de máquinas, neste grupo de ativos a maior vulnerabilidade encontrada está na sensibilidade à umidade, poeira e sujeira, não só por conta dos resíduos naturais ocasionados da movimentação de documentos e da utilização dos ativos, mas porque possuí uma caixa d'água, que serve para abastecimento, em caso de uma eventual falta de água. As máquinas não ficam diretamente em contato com o chão, mas em caso de uma ruptura deste reservatório de água, mesmo que baixo, seria possível algum dano aos ativos de TI neste andar.

Tabela 8 - Vulnerabilidades Ativos Segundo Andar

Ativo	Vulnerabilidades	Ameaças	Risco
Switch	Uso inadequado ou sem os cuidados necessários dos mecanismos de controle do acesso físico a prédios e salas	Destruição de equipamento ou mídia	O segundo andar perderá a comunicação com a rede
Switch	Falta de uma rotina de substituição periódica	Destruição de equipamento ou mídia	O segundo andar perderá a comunicação com a rede
Nobreak	Sensibilidade à umidade, poeira, sujeira	Poeira, corrosão, congelamento	Em caso de queda de Energia, O primeiro andar perderá a comunicação com a rede
Nobreak	Falta de uma rotina de substituição periódica	Destruição de equipamento ou mídia	Em caso de queda de Energia, O primeiro andar perderá a comunicação com a rede

Ativo	Vulnerabilidades	Ameaças	Risco
Relógio Ponto	Inexistência de mecanismos estabelecidos para o monitoramento de violações de segurança	Furto de mídia ou documentos	Em caso de dano ao relógio ponto, ou quebra da integridade do equipamento, não há um registro desta ocorrência
Relógio Ponto	Fornecimento de Energia Instável	Interrupção do Serviço de Energia	Não registradas as entradas de funcionários
Impressora	Fornecimento de Energia Instável	Interrupção do Serviço de Energia	Máquinas do Segundo andar não poderão realizar impressão
Impressora	Sensibilidade à umidade, poeira, sujeira	Poeira, corrosão, congelamento	indisponibilidade ou quebra do equipamento
Desktops	Não execução do *logout* ao se deixar uma estação de trabalho desassistida	Abuso de direitos	Acesso não autorizado
Desktops	Atribuição errônea de direitos de acesso	Abuso de direitos	Todos os usuários possuem Permissão de administrador
Desktops	Fornecimento de Energia Instável	Interrupção do Serviço de Energia	Todas as máquinas estão indisponíveis

Fonte: Próprio Autor

Dentro dos ativos listados na tabela 8, existe o Relógio Ponto do escritório, com a funcionalidade de registrar os horários de entradas e saídas dos funcionários, portanto um ativo muito importante, porem o mesmo não possuí um fornecimento de energia reserva. Outro ponto importante que deve ser ressaltado é a falta de monitoramento até o acesso do relógio ponto. Caso um funcionário realize algum ato

que venha ferir a integridade deste ativo, como quebra do ativo, ou utilizar de ferramentas que venha alterar seus horários de entradas e saídas, isto não poderá ser fiscalizado.

Tabela 9 - Vulnerabilidades Ativos Terceiro Andar

Ativo	Vulnerabilidades	Ameaças	Risco
Servidor de *Backup*	Uso inadequado ou sem os cuidados necessários dos mecanismos de controle do acesso físico a prédios e salas	Destruição de equipamento ou mídia	Perda das Cópias de Segurança
Servidor de *Backup*	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de mídia ou documentos	Porta de acesso a sala do Servidor, não é segura
Servidor de *Internet*	Uso inadequado ou sem os cuidados necessários dos mecanismos de controle do acesso físico a prédios e salas	Destruição de equipamento ou mídia	Escritório ficará Offline
Servidor de *Internet*	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de mídia ou documentos	Escritório ficará Offline Temporariamente
Servidor de *Internet*	Inexistência de um plano de continuidade	Falha de equipamento	Escritório ficará Offline Temporariamente

Ativo	Vulnerabilidades	Ameaças	Risco
Host VM	Inexistência de mecanismos de proteção física no prédio, portas e janelas.	Furto de mídia ou documentos	Parte dos serviços do Escritório ficará Offline
Host VM	Uso inadequado ou sem os cuidados necessários dos mecanismos de controle do acesso físico a prédios e salas	Destruição de equipamento ou mídia	Parte dos serviços do Escritório ficará Offline
Nobreak 1	Falta de uma rotina de substituição periódica	Destruição de equipamento ou mídia	Em caso de queda de Energia, os equipamentos serão desligados de forma insegura
Nobreak 1	Sensibilidade à umidade, poeira, sujeira.	Poeira, corrosão, congelamento.	Em caso de queda de Energia, O primeiro andar perderá a comunicação com a rede
Nobreak 2	Falta de uma rotina de substituição periódica	Destruição de equipamento ou mídia	Em caso de queda de Energia, os equipamentos serão desligados de forma insegura
Nobreak 1	Falta de uma rotina de substituição periódica	Destruição de equipamento ou mídia	Em caso de queda de Energia, os equipamentos serão desligados de forma insegura
Switch	Falta de uma rotina de	Destruição de	Os *hosts* não poderão

	substituição periódica	equipamento ou mídia	acessar os Servidores
Repetidor	Falta de uma Rotina de Substituição Periódica	Destruição de equipamento ou mídia	Diminui a qualidade da rede visitante
Nobreak	Sensibilidade à umidade, poeira, sujeira	Poeira, corrosão, congelamento	Em caso de queda de Energia, Todos os andares perdem a comunicação com a rede
Central de Alarme	Sensibilidade à umidade, poeira, sujeira	Poeira, corrosão, congelamento	em caso de mal funcionamento a não tem monitoramento a invasão/roubo
Roteador	Falta de uma Rotina de Substituição Periódica	Destruição de equipamento ou mídia	Colaborador não poderá conectar no *wifi*
Roteador	Fornecimento de Energia Instável	Interrupção do Serviço de Energia	Colaborador não poderá conectar no *wifi*
Desktops	Localização em área suscetível a inundações	Inundação	Máquinas Danificadas por inundação
Desktops	Não execução do logout ao se deixar uma estação de trabalho desassistida	Abuso de direitos	Acesso não autorizado
Desktops	Atribuição errônea de direitos de acesso	Abuso de direitos	Todos os usuários possuem Permissão de administrador
Desktops	Fornecimento de Energia Instável	Interrupção do Serviço de Energia	Todas as máquinas estão indisponíveis

Ativo	Vulnerabilidades	Ameaças	Risco
Notebooks	Atribuição errônea de direitos de acesso	Abuso de direitos	Todos os usuários possuem Permissão de administrador
Impressora	Fornecimento de Energia Instável	Interrupção do Serviço de Energia	Máquinas do Segundo andar não poderão realizar impressão
Impressora	Sensibilidade à umidade, poeira, sujeira	Poeira, corrosão, congelamento	indisponibilidade ou quebra do equipamento
Link de comunica-ção	Acordo de Nível de Serviço (ANS/SLA) inexistente ou insuficiente	Violação das condições de uso do sistema de informação que possibilitam sua manutenção	Escritório ficará sem conexão externa temporariamente

Fonte: Próprio Autor

O Terceiro andar é o local que possui os principais ativos de TI, conforme apresentado na tabela 9, onde estão localizados os servidores, Link de Comunicação e central de alarme. Um dos principais problemas é o fácil acesso até estes ativos.

Tabela 10 - Vulnerabilidades Ativos *Offline*

Ativo	Vulnerabilidades	Ameaças	Risco
Documentos Contábeis	Inexistência de procedimentos para a manipulação de informações classificadas	Erro durante o uso	Não há registros de controles. Em caso de perda de algum documento, não há nenhuma rastreabilidade.

Ativo	Vulnerabilidades	Ameaças	Risco
Documentos Contábeis	Inexistência de cópias de segurança (*back-up*)	Furto de mídia ou documentos	Não há maneiras de recuperar documentos perdidos
Documentos Fiscais	Inexistência de procedimentos para a manipulação de informações classificadas	Erro durante o uso	Não há registros de controles. Em caso de perda de algum documento, não há nenhuma rastreabilidade.
Documentos Fiscais	Inexistência de cópias de segurança (*back-up*)	Furto de mídia ou documentos	Não há maneiras de recuperar documentos perdidos
Documentos Trabalhistas	Inexistência de procedimentos para a manipulação de informações classificadas	Erro durante o uso	Em caso de perda de algum documento, não há nenhuma rastreabilidade, e haverá prejuízo financeiro ao escritório.
Documentos Trabalhistas	Inexistência de cópias de segurança (*back-up*)	Furto de mídia ou documentos	Não há maneiras de recuperar documentos perdidos
Documentos Societários	Inexistência de procedimentos para a manipulação de informações classificadas	Erro durante o uso	Em caso de perda de algum documento, não há nenhuma rastreabilidade, e haverá prejuízo financeiro ao escritório

Ativo	Vulnerabilidades	Ameaças	Risco
Documentos Societários	Inexistência de cópias de segurança (*back-up*)	Furto de mídia ou documentos	Não há maneiras de recuperar documentos perdidos

Fonte: Próprio Autor

Conforme descrito no tópico 4.1.2, no grupo de ativos de *offline,* há muitos documentos físicos, que se sofrerem danos aos mesmos, não haverá formas de recuperar, podendo gerar prejuízo ao escritório e aos seus clientes.

4.3 ANÁLISE QUANTITATIVA DOS RISCOS

Após a realização do levantamento de ativos e vulnerabilidades apresentadas neste ambiente, também foi realizada uma análise quantitativa para medir o grau de risco de cada ativo. Conforme Bezerra, (2013), em seu estudo sobre a norma NBR 27005:

> "[...] Na metodologia da análise quantitativa é utilizada uma escala de valores numéricos com objetivo de tentar calcular valores numéricos para cada um dos componentes coletados durante as atividades de identificação de riscos..[...]"

Para a realização desta Análise quantitativa dos Riscos, os Ativos foram novamente organizados por andares, e utilizado o calculo a seguir para definir quais ativos estão com maior risco.

Cálculo utilizado para obter o valor do Risco:
QualAV = Confidencialidade + Integridade + Disponibilidade
Valor do Risco = QualAV * Probabilidade * Impacto

Quanto ao cálculo para esta definição, foi utilizado o seguinte critério:

Confidencialidade (*Confidentiality* - C): O valor da confidencialidade descreve o quão importante os ativos são e quais devem permanecer confidenciais, garantindo que a informação seja acessível somente para aqueles que contém autorização de

acesso. A confidencialidade pode ser classificada em seis valores: Não aplicável (0), não confidencial (1), não muito confidencial (2), confidencial (3), muito confidencial (4) e altamente confidencial (5).

Integridade (*Integrity* - I): Integridade significa que a informação é a mesma e não foi alterada, nem ativamente nem passivamente. O valor da integridade descreve como é importante que a integridade dos ativos sejam protegidas, e são classificadas em cinco tipos: Não aplicável (0), muito baixo (1), baixo (2), médio (3) e alto (4).

Disponibilidade (*Availability* – A): Disponibilidade significa que um ativo está a serviço dos usuários, e o valor da disponibilidade descreve o quão importante do recurso estar disponível e é classificada em seis tipos: Não aplicável (0), sem importância (1), não muito importante (2), importante (3), muito importante (4) e extremamente importante (5).

Valor Patrimonial Qualitativo (QualAV): Indica o grau de necessidade do ativo atender os pilares da Segurança da Informação.

Probabilidade (*Likelihood* – L): A probabilidade descreve o quão provável é a exploração de uma vulnerabilidade. Pode-se classificar em seis valores: Não aplicável (0), muito improvável (1), improvável (2), possível (3), provável (4) e muito provável (5).

Impacto (*Impact* – I): O impacto descreve o resultado do quão ruim quando uma vulnerabilidade é explorada gerando uma indisponibilidade do ativo: Muito baixo (1), Baixo (2), Normal (3), Alto (4), Muito Alto (5).

Fonte dos cálculos retiradas do material utilizado em sala de aula do professor Edson Roberto Gaseta, matéria de Gestão de Risco, 2017.

As tabelas a seguir (tabelas de 11 a 15) contém os resultados obtidos pela análise quantitativa. Novamente os ativos foram organizados por andares.

Tabela 11 Análise Quantitativa Ativos Térreo

Ativos	Confi.	Integr	Dispo	Qual AV	Proba.	Impacto	Valor do Risco
Stand Alone DVR	4	4	4	12	3	1	36
Roteador	2	0	5	7	3	3	63
Notebook	3	4	4	11	3	1	33

Fonte: Próprio Autor

Tabela 12 Análise Quantitativa Ativos Primeiro Andar

Ativos	Confi.	Integri	Dispo.	Qual AV	Proba.	Impacto	Valor do Risco
Switch	0	0	5	5	3	5	75
Nobreak	0	0	5	5	1	2	10
Desktops	3	4	5	12	3	4	144
Notebook	3	4	4	11	3	4	132
Impressora	0	0	3	3	3	1	9

Fonte: Próprio Autor

Tabela 13 Análise Quantitativa Ativos Segundo Andar

Ativos	Confi.	Integri	Dispo.	Qual AV	Proba.	Impacto	Valor do Risco
Switch	0	0	5	5	3	5	75
Nobreak	0	0	5	5	1	2	10
Relógio Ponto	5	4	5	14	3	4	168
Impressora	0	0	3	3	3	1	9
Desktops	3	4	5	12	3	4	144

Fonte: Próprio Autor

Tabela 14 Análise Quantitativa Ativos Terceiro Andar

Ativos	Confi.	Integri	Dispo.	Qual AV	Proba.	Impacto	Valor do Risco
Servidor de *Backup*	5	4	5	14	3	4	168
Servidor de *Internet*	5	4	5	14	3	4	168
Host VM	5	4	5	14	3	5	210
Nobreak 1	0	0	5	5	3	4	60
Nobreak 2	0	0	5	5	3	4	60
Switch	0	0	5	5	3	5	75
Repetidor	2	0	5	7	3	3	63
Central de Alarme	2	4	5	11	2	4	88
Roteador	5	4	1	10	3	1	30
Desktops	3	4	5	12	3	4	144
Nobreak	0	0	5	5	1	2	10
Notebooks	3	4	4	11	3	4	132
Impressora	0	0	3	3	3	1	9
Link Comunicação	0	0	5	5	2	4	40

Fonte: Próprio Autor

O Terceiro andar é o local com mais ativos, e sua análise qualitativa dos riscos apontam que o ativo com maior índice de risco é o *Host VM* com um índice de risco de 210 conforme a tabela 14.

Tabela 15 Análise Quantitativa Ativos *Offline*

Ativo	Confi.	Integri	Dispo.	Qual AV	Proba.	Impacto	Valor do Risco
Documentos Contábeis	5	4	5	14	3	4	168
Documentos Fiscais	5	4	5	14	3	3	126
Documentos Trabalhistas	5	4	5	14	4	5	280
Documentos Societários	5	4	5	14	3	5	210

Fonte: Próprio Autor

Com a análise dos ativos *offline* é possível identificar que possuí ativos não digitais que estão sob um risco maior que ativos de TI. O que leva a entender que se torna necessário uma tratativa também para estes ativos, por serem dados tão sensíveis, e estarem sob tão risco.

4.4 LEVANTAMENTO DA PRIORIZAÇÃO DOS RISCOS

Conforme o levantamento da Análise Qualitativa, e aos dados obtidos no levantamento, foi apontado oito ativos com índice de risco superior a 130, e que serão abordados para uma proposta de melhoria. Na tabela 16, é possível identificar os ativos, e seus respectivos resultados da análise qualitativa.

Tabela 16 Ativos com maior índice de risco

Ativos	Confi.	Integri	Dispo.	Qual AV	Proba.	Impacto	Valor do Risco
Documentos Trabalhistas	5	4	5	14	4	5	280
Host VM	5	4	5	14	3	5	210
Documentos Societários	5	4	5	14	3	5	210
Servidor de *Internet*	5	4	5	14	3	4	168

Ativos	Confi.	Integri	Dispo.	Qual AV	Proba.	Impacto	Valor do Risco
Documentos Contábeis	5	4	5	14	3	4	168
Relógio Ponto	5	4	5	14	3	4	168
Desktops	3	4	5	12	3	4	144
Notebook	3	4	4	11	3	4	132

Fonte: Próprio Autor

5 PROPOSTA DE MELHORIA

Com todo este levantamento dos problemas de segurança neste ambiente estudado, foi possível caracterizar os principais ativos que estão sob maior risco, o que permite realizar uma proposta de tratamento dos riscos atuais.

Com base neste estudo de caso, e informações levantadas, foi realizada uma proposta de melhoria, apoiada nos critérios abaixo, a fim de retirar, ou mitigar o risco. A proposta de melhoria será indicada a fim de mitigar os ativos com maior risco, apontados pela análise quantitativa, mesmo que não necessariamente sejam aplicadas somente a eles. Ou seja, com as vulnerabilidades e risco dos principais ativos, é possível elaborar melhorias fundamentadas nos pilares da segurança da informação não só agregando tecnologia mais criando normas, procedimentos e boas práticas para ter então um ambiente com maior segurança.

A implantação de algumas medidas de melhorias pode garantir os pilares da segurança da informação, medidas essas que apesar de variar em valores, são relativamente fáceis de manutenção e aplicação, portanto este trabalho buscou através de um *framework* de cibersegurança oferecer melhorias que trariam impactos aos níveis de risco e probabilidades no ambiente da contabilidade.

O *framework* utilizado é disponibilizado pelo *The National Institute of Standards and Technology* (NIST), ele oferece não só controles mais todo uma metodologia de gestão e monitoramento da segurança da informação, onde dentro dele se tem acesso aos mais diferentes tipos de controles como COBIT, ISO 27001 entre outros. Este trabalho tomou como base os tópicos de controles de segurança dispostos nos NIST SP 800-53 Rev. 4.

5.1 IMPLEMENTAÇÃO DE CONTROLE DE MOVIMENTAÇÃO DE DOCUMENTOS

Com relação a documentação física existente, o que abrange documentos trabalhistas, societários, contábeis, fiscais, entre outros, existem riscos como o extravio ou a deterioração da documentação, também existe o fator de não rastreabilidade e versionamento dos documentos o que pode causar prejuízo financeiro ao escritório ou aos seus clientes.

A Implantação de um sistema gestor eletrônicos de documentos (GED) pode aplicar controles de entradas e saídas de documentos, possibilitando rastreamento e

versionamento dos dados.

Se o sistema GED for aplicado aos documentos físicos, os controles e resultados podem ser potencializados pelo fato da diminuição de contato físico dos usuários com os documentos, além de ampliar as possibilidades de transações e troca de documentos entre o cliente e contador, pois a comunicação eletrônica digital seria a principal via de troca de documentos.

Esta melhoria entra nos seguintes controles do *framework* do NIST: AC-1, AU-4, CA-1, MA-3.

5.2 MEDIDAS DE CONTINUIDADE

Com relação aos ativos de TI como os computadores e notebooks, sobretudo os servidores, existe a possibilidade de parada de funcionamento que pode interromper em 100% a produtividade ou a disponibilidade dos serviços e funcionamento do empreendimento, deixando o ambiente offline em vários quesitos, como sistemas, comunicação etc.

Após analisar os itens de controle do NIST como CP-10 ou o PE-9 é possível identificar que tipos de melhorias devem se aplicadas para garantir a disponibilidade do ambiente contábil, sendo algumas delas a redundância de ativos chaves como servidores e links de internet, além da implantação e manutenção dos sistemas de backup dos ativos informatizados (sistemas, PDF e outros arquivos pertinentes), e para auxiliar na continuidade Nobreaks para os principais dispositivos da rede como máquina dos coordenadores e diretoria.

5.3 MEDIDAS DE CONTROLE DE ACESSO:

Como normalmente um ambiente físico de um escritório contábil atende a necessidade de ter diversos colaboradores e a capacidade de receber clientes e terceiros, existe o risco de que indivíduos tenham acesso a áreas restritas e proporcionem alterações nos status ou qualidade dos serviços e ativos, podendo proporcionar a parada total ou indisponibilidade parcial de algum ativo físico ou virtual, por exemplo os servidores.

Dentro do *framework* do NIST, existem controles como PE-3 que demonstram a importância do controle de acesso físico a todos os ativos, como máquinas e

documentos. É possível identificar que as seguintes medidas devem ser implementadas para suprir a necessidade de um controle de acesso: Política de controle de acesso, Política de acompanhamento de terceiros, Política de sigilo de informações e controles internos, Mecanismos de vigilância e Mecanismos de controles de acessos.

A aplicação de controles de acesso às áreas restritas como arquivo, almoxarifado, ou até mesmo a ativos como servidores, roteadores e relógio ponto. podem proporcionar a disponibilidade do escritório, contudo além do controle de acesso físico garantir a autenticidade das pessoas é fundamental, por isso políticas e treinamentos também devem ser levados em consideração, em outras palavras a aplicação de todos os itens destacados acima poderiam proporcionar um controle de acesso aos ativos e setores com maior confiabilidade e facilidade.

5.4 SEGURANÇA A USUÁRIOS:

Com a diversificação de máquinas no parque computacional e atividades desempenhadas pelos colaboradores, existe o risco de que os usuários compartilhem senhas ou disponibilizem seus acessos restritos a utilização temporária para outros indivíduos não autorizados, ferindo o pilar de autenticidade e disponibilidade da segurança da informação.

De acordo com alguns controles do NIST, monitorar e treinar os usuários é essencial como demonstra o controle AT-1, portanto aplicar esse controle pode trazer resultados. Contudo exige uma mudança de hábito nem sempre aceita pelo ambiente, e mediante a isso, medidas de contorno a potenciais problemas na exploração das vulnerabilidades devem ser aplicadas para mitigar os riscos. Algumas medidas como:

- Política de troca de senhas.
- Política de iniciação de usuários novos.
- Política de desligamento de usuários e senhas.
- Retirada de privilégios e acessos concedidos indevidamente aos usuários à sistemas e a ativos de TI.

5.5 MEDIDAS DE SEGURANÇA OU DE DISPOSIÇÃO FÍSICA DOS ATIVOS:

Mesmo com controles de acessos e mecanismos que garantem a autenticidade de acesso a um ativo, existe a possibilidade ocorrer um dano físico ou devido a uma má gestão diminuir sua qualidade ou a sua vida útil tanto de documentos quanto de equipamentos e ativos de TI. Mediante essa situação reestruturar ativos que possam ser impactados com algum tipo de influência física externa é essencial, como por exemplo:

- Reinstalação física adaptada de máquinas com algum tipo de influência externa perigosa (exposição a sujeira extrema, a água ou produtos químicos como produtos de limpeza).
- Políticas sobre danos causados a equipamentos e documentos pelos usuários.
- Políticas de empacotamento de documentos e ativos de TI.

Essas medidas de segurança são justificadas pelo NIST através dos tópicos PE-14, PE-15, PE-18

5.6 RESULTADO DAS MELHORIAS

Para melhor organização e compreensão da proposta, os ativos foram correlacionados com o resultado de sua Análise Qualitativa, Riscos apresentados, Tratamento do Risco e Aceitação do Risco. Tendo como suposição de que toda a proposta foi implementada com sucesso, espera-se obter uma redução. Na tabela 17, é realizada uma nova análise qualitativa após a implementação.

Tabela 17 - Análise Quantitativa após a Implementação da Proposta

Ativos	Confi.	Integri	Dispo.	Qual AV	Prob.	Impacto	Valor do Risco
Documentos Trabalhistas	5	4	5	14	3	4	168
Host VM	5	4	5	14	2	5	140
Documentos Societários	5	4	5	14	3	4	168
Servidor de *Internet*	5	4	5	14	2	4	112

Ativos	Confi.	Integri	Dispo.	Qual AV	Prob.	Impacto	Valor do Risco
Documentos Contábeis	5	4	5	14	2	4	112
Relógio Ponto	5	4	5	14	2	3	84
Desktops	3	4	5	12	2	4	96
Notebook	3	4	4	11	2	4	88

Fonte: Próprio Autor

Em seguida na tabela 18, consta um comparativo entre os ativos que estão com maior índice de risco, com a redução que se espera obter caso a proposta seja implantada com sucesso.

Tabela 18 - Redução em (%) em cada Ativo

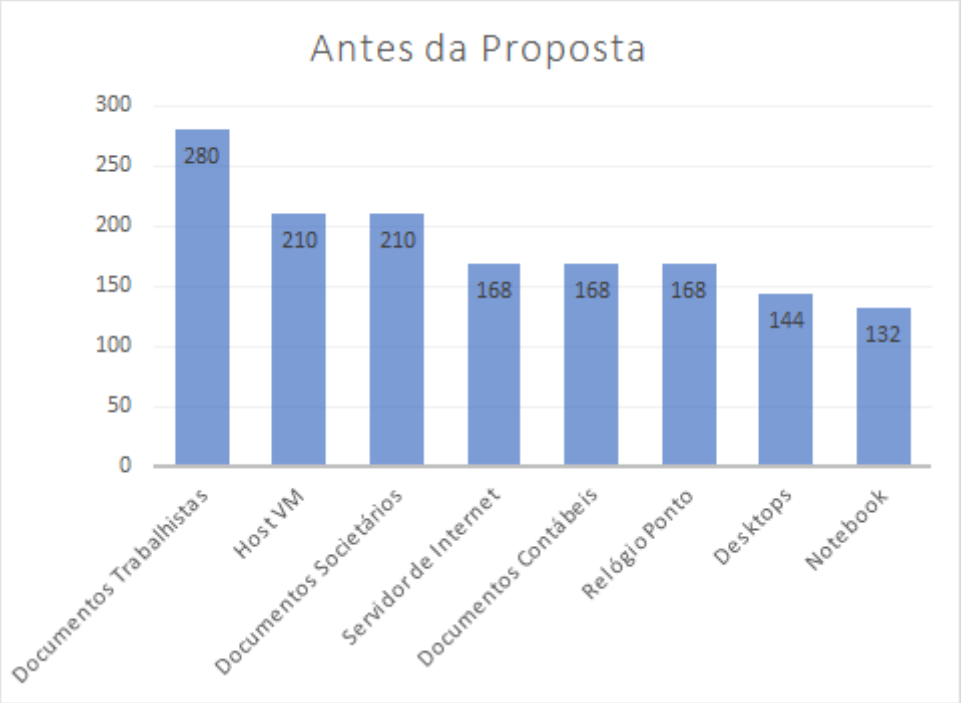
Ativos	Valor do Risco Ant.	Valor do Risco Atual	Redução do Risco %
Documentos Trabalhistas	280	168	40
Host VM	210	140	33,34
Documentos Societários	210	168	20
Servidor de *Internet*	168	112	33,34
Documentos Contábeis	168	112	33,34
Relógio Ponto	168	84	50
Desktops	144	96	33,34
Notebook	132	88	33,34
Média da Redução	**34,59%**		

Fonte: Próprio Autor

Como apontado pela tabela 18, sendo implementada a proposta de melhoria, é esperado obter uma redução de 34,59% no índice de risco dos ativos tratados, e o ativo que se espera obter maior redução em seu índice de risco é o Relógio ponto, onde sua redução é de 50%.

O gráfico exibido na Figura 2 aponta o valor do risco dos ativos que obtiveram maior índice de risco conforme a análise quantitativa antes da implementação da proposta de melhoria:

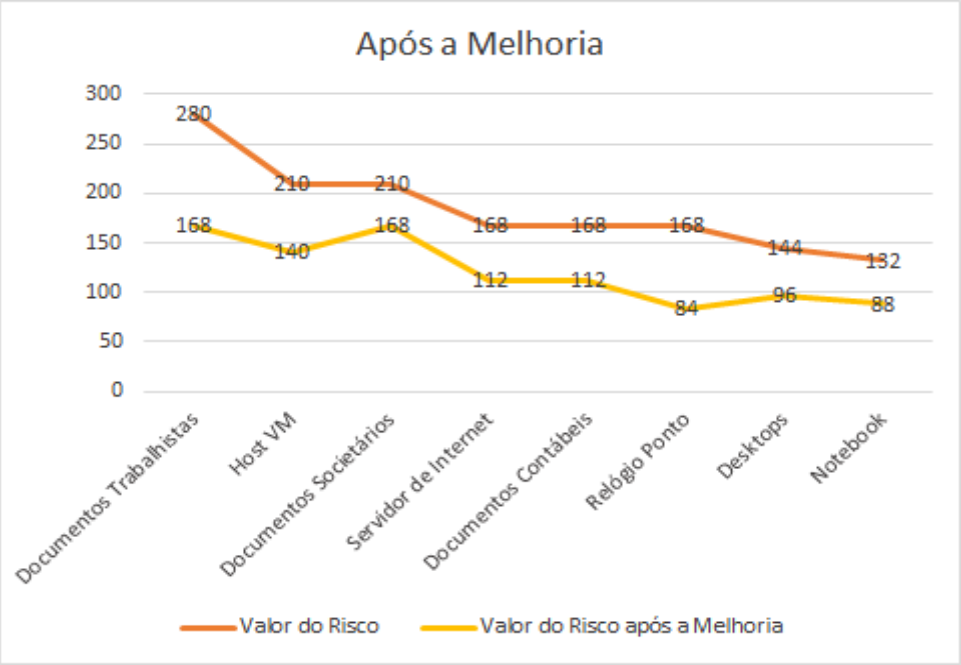
Figura 2 - Valor de risco antes da implementação da proposta de melhoria



Fonte: Próprio Autor

Em seguida a Figura 3, compara os valores de risco de cada ativo após a implementação da proposta de melhoria.

Figura 3 Comparação entre os valores de risco antes e depois da proposta de melhoria



Fonte: Próprio Autor

Com a visualização destes gráficos é possível identificar o resultado da redução do valor do risco dos ativos com maior índice segundo a análise qualitativa, que se espera obter com a implementação da proposta de melhoria.

6 CONSIDERAÇÕES FINAIS

Através dos estudos realizados nesse trabalho, é possível chegar principalmente em três conclusões fundamentais. Primeiramente e principalmente é possível concluir que as informações que transitam entre o ambiente contábil e o empresarial são extremamente sensíveis, e se disponibilizadas a acessos indevidos ou a concorrentes, podem ocasionar impactos sérios ao ambiente contábil e seus clientes, ou seja a confidencialidade dessa informação deve ser vista como prioridade nas tomadas de decisão e investimentos, Devido ao grau de sensibilidade das informações cuidados com o gerenciamento e o resguardo das mesmas também tem que ser analisadas e gerenciadas.

A segunda conclusão é que a evolução da informática não prejudica o setor, pelo contrário, através dela o setor contábil agrega aos seus serviços e portfólios qualidade e produtividade, focando sua mão de obra em atividades analíticas no *core* empresarial de seu negócio. Contudo, esses recursos tecnológicos necessitam de uma aplicação e sobretudo uma gestão eficiente, para que os resultados agregados sejam efetivos e sem afetar o ambiente com abrangências de vulnerabilidades. Mesmo com recursos para redução de processos a informação processada é o ativo principal da contabilidade, e por isso deve ser sempre visado quais impactos e melhorias a introdução de novos serviços e tecnologias.

Por fim, a terceira conclusão é que durante este estudo de caso foi possível analisar tudo o ambiente contábil e compreender as rotinas e necessidades que o mesmo possui para realizações de suas atividades. Foi possível analisar um ambiente real, onde o mesmo apresentava alguns riscos, e através de simples modificações, foi possível obter uma redução de 34% do índice de risco nos oito ativos tratados na análise inicial.

Com o ambiente tratado durante este estudo, é possível utilizá-lo como exemplo prático para outros ambientes contábeis, pois os mesmos possuem em tese, as mesma obrigatoriedades e as mesmas rotinas, diferenciando em sua instalação, quantidades de ativos, ou grau de sensibilidade das informações , ou ainda uma ligeira variação nos sistemas e no gerenciamento dos recursos *offline* ou ativos de TI, quantidade do corpo de funcionários e a quantidade de clientes atendidos.

Concluindo que a mesmo com a variação de algumas situações, ainda é possível avaliar de forma generalizada que ambientes contábeis encontram uma dificuldade em aplicar uma gestão e instalação de recursos de forma eficiente e menos propensa a exploração de ameaças.

REFERÊNCIAS BIBLIOGRÁFICAS

BEZERRA, Edson Kowask**. Gestão de Risco de TI:** NBR 27005. 2. ed. Rio de Janeiro: Escola Superior de Redes, 2013. 19 - 101 p

BRASIL. RECEITA FEDERAL. . **SPED:** APRESENTAÇÃO. 2007. Disponível em: <http://sped.rfb.gov.br/pagina/show/964>. Acesso em: 18 maio 2019.

LUCAS, Douglas Ribeiro. **A VALORIZAÇÃO DO PROFISSONAL CONTÁBIL E OS BENEFÍCIOS PARA A CONTABILIDADE, ATRAVÉS DO AVANÇO DA TECNOLOGIA DA INFORMAÇÃO.** 2009. 5 f. TCC (Graduação) - Curso de Ciências Contábeis, Facesm, Itajubá, 2009.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **SP 800-53 REV. 4**: Security and Privacy Controls for Federal Information Systems and Organizations. 4 ed. 2013. 462 p. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>. Acesso em: 02 junho 2019.

OMIE (Brasil). **Mercado contábil na atualidade**: Desafios e oportunidades. 2015. Disponível em: <https://blog.omie.com.br/blog/mercado-contabil-atualidade-desafios-e-oportunidades>. Acesso em: 18 maio 2019.

OSAYK (Brasil). **Quais são as obrigações contábeis, fiscais e previdenciárias das empresas?** 2019. Disponível em: <https://osayk.com.br/quais-sao-as-obrigacoes-contabeis-fiscais-e-previdenciarias-das-empresas/>. Acesso em: 18 maio 2019.

PORTAL DA CONTABILIDADE (Brasil). **ESCRITÓRIO DE CONTABILIDADE:** ANÁLISE DE NEGÓCIO. 2006. Disponível em: <http://www.portaldecontabilidade.com.br/tematicas/escritorio.htm>. Acesso em: 18 maio 2019.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** Uma visão executiva. 2. ed. Rio de Janeiro: Elsevier Editora Ltda, 2014. 68 - 69 p.

WOLTERS KLUWER (Brasil). **Como aumentar a segurança e agilidade em transações contábeis na nuvem?** 2019. Disponível em:

<http://www.wolterskluwer.com.br/blog/contabilidade-colaborativa/>. Acesso em: 18 maio 2019.