UNIVERSIDADE DE CAXIAS DO SUL

TATIELI ZANELLA

ESTUDO SOBRE A QUEBRA DE CONFIDENCIALIDADE DA INFORMAÇÃO E MECANISMOS DE SEGURANÇA

CAXIAS DO SUL

2017

TATIELI ZANELLA

ESTUDO SOBRE A QUEBRA DE CONFIDENCIALIDADE DA INFORMAÇÃO E MECANISMOS DE SEGURANÇA

Trabalho de conclusão do curso de graduação, apresentado ao Centro de Ciências Exatas e de Tecnologia da Universidade de Caxias do Sul, como requisito para a obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Prof. Maria de Fátima Webber do Prado Lima

CAXIAS DO SUL

2017

Dedico este trabalho aos meus preciosos pais Dolores e Marcelino, por toda dedicação, incentivo e amor.

AGRADECIMENTOS

Agradeço primeiramente à Deus, pela vida, pelas pessoas especiais que colocaste em meu caminho, por estar presente em todos os momentos da minha vida, concedendo-me força para alcançar meus sonhos.

Meu agradecimento de forma especial aos meus pais Dolores e Marcelino e meu irmão Tiago que, além do carinho e incentivo, possibilitaram a realização desta conquista em minha vida. Por entenderem os vários momentos ausentes para dedicação aos estudos.

Agradeço ao meu noivo Rafael, pelo amor e compreensão pela minha ausência em determinados momentos. Por ser a minha base em todos os momentos desta caminhada, principalmente nestes últimos meses e por estar sempre presente. Por toda a ajuda que dedicaste a mim.

À minha orientadora Prof. Maria de Fátima Webber do Prado Lima, pela orientadora dedicada e competente que és e por sua significativa contribuição durante todo o desenvolvimento desta monografia.

Agradeço à empresa de São Marcos, em especial o diretor, que permitiu aplicar este estudo fornecendo todos os dados necessário para o bom andamento. Agradeço também aos funcionários pela colaboração ao responderem os questionários propostos.

Agradeço profundamente aos meus amigos e a todos que, direta ou indiretamente, me apoiaram nesta caminhada, sendo, com certeza, o combustível da minha vida.

“ A tarefa não é tanto ver aquilo que ninguém viu, mas pensar o que ninguém ainda pensou sobre aquilo que todo mundo vê”.

Arthur Schopenhauer

RESUMO

Com a evolução da tecnologia, as informações passaram de processos manuais para processos automatizados. Com estas mudanças, a informação necessitava da garantia de ser gerada através de sistemas e ao mesmo tempo fosse íntegra, confiável e segura. A partir dos momentos em que uma informação é criada, é de grande importância que esta informação seja protegida. Dentro das organizações a informação é um dos bens mais valiosos que ela possui e, por esta razão, é comum enfrentar diversos obstáculos, tais como, ameaças, vulnerabilidades e ataques a este ativo. Há, então, uma série de mecanismos de segurança e ferramentas que podem ser montadas como barreira para impedir os elos entre a informação e suas ameaças. O objetivo geral deste trabalho foi sistematizar os principais tipos de ataques, mecanismos de segurança e ferramentas relacionados com a quebra de confidencialidade que podem ocorrer dentro de uma organização. Os resultados deste estudo foram aplicados em uma empresa de pequeno porte a fim de auxiliar na proteção da confidencialidade dos dados. O estudo de caso mostrou que mesmo em uma empresa pequena é necessário criar uma cultura de segurança e ferramentas de proteção dos dados.

Palavras-chave: Confidencialidade; Ameaças; Mecanismos de Segurança; Ferramentas;

ABSTRACT

With the evolution of technology, the information has gone from manual processes to automated processes. With these changes, the information required the assurance of being generated through systems while being complete, reliable and secure. From the moment when the information is created, it is of great importance that this information is protected. Within organizations, information is one of the most valuable assets it possesses, and for this reason, it is common to face several obstacles, such as threats, vulnerabilities and attacks on this asset. There are, then, a number of security mechanisms and tools that can be set up as a barrier to prevent links between information and its threats. The general objective of this work was to systematize the main types of attacks, security mechanisms and tools related to the breach of confidentiality that can occur inside an organization and to elaborate an operational strategy to protect the confidentiality of the data. The results of this study were applied to a small business in order to assist in the protection of data confidentiality. The case study has shown that even in a small business it is necessary to create a culture of security and tools of data protection.

Keywords: Confidentiality; Threats; Security Mechanisms; Tools;

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CEF	Caixa Econômica Federal
CIA	*Confidentiality, Integrity and Availability*
IDS	*Intrusion Detection System*
iOS	*iPhone Operating System*
MAC OS	*Macintosh Operating Systems*
SET	*Secure Electronic Transaction*
SQL Injections	*Structured Query Language*
SSL	*Secure Socket Layer*

SUMÁRIO

1. INTRODUÇÃO

É sabido que a facilidade na troca de informação tem evoluído de uma maneira muito rápida, porém essa facilidade na comunicação mundial gera um problema: o acesso indevido a essas informações e a falta de confiabilidade dos dados.

Diante desta realidade, a Segurança da Informação tornou-se um assunto muito abordado e comentado nos últimos tempos e tem sido, mais do que nunca, uma ferramenta primordial para tomadas de decisões estratégicas em todos os setores da sociedade. Isto se deve, pois, a quebra de confidencialidade ou a análise equivocada da informação pode tornar-se uma grande vilã para as organizações quando usada inapropriadamente ou sem autorização.

Como tendência, as organizações deverão mudar seu enfoque em relação a segurança da informação priorizando, não apenas as ferramentas de prevenção contra-ataques, mas sim os dados produzidos e coletados dentro da empresa. Segundo um estudo conduzido pelo Instituto Ponemon em parceria com a Varonis, descobriu-se que 62% dos funcionários afirmam que possuem acesso a dados que não seriam necessários para realizar suas tarefas diárias. Ainda, menos de 30% das empresas possuem registros do que seus funcionários estão fazendo com as informações (COMPUTERWORLD, 2016).

Em agosto de 2013, o Yahoo teve o maior vazamento de dados da história onde afirma que dados associados a mais de um bilhão de contas de usuários foram roubados, entre eles, nomes, endereços de e-mail, números telefônicos, datas de nascimento e senhas criptografadas (COMPUTERWORLD, 2016).

Também em 2013, mais de 4,6 milhões de usuários do aplicativo Snapchat receberam uma notificação de que seus números de celulares e localização foram divulgados sem suas permissões (LANDIM, 2014).

Outra brecha na base de dados da T-Mobile nos EUA ocasionou a exposição de dados de 15 milhões de consumidores norte-americanos ligados à operadora entre setembro de 2013 e setembro de 2015. Foram roubadas informações pessoais como nomes, endereços, números do Seguro Social, número de carteira de motorista e outros (COMPUTERWORL, 2015).

Além disso, outro caso mais antigo, porém não menos importante. Entre 2006 e 2008, a empresa Heartland especializada em pagamentos, sofreu um problema de *SQL Injections* (códigos que se comunicam diretamente com o banco de dados), onde permitiu aos *hackers* roubarem dados de pagamento de aproximadamente 130 milhões de cartões de crédito e débito.

Visto de outra forma, sem a informação ou com a informação distorcida, o negócio pode ter perdas incalculáveis que afetam o seu funcionamento normal e o retorno de investimentos da empresa. A segurança da informação existe para minimizar os riscos do negócio em relação à dependência do uso dos recursos de informação para o funcionamento da organização (FONTES, 2006).

Adotam-se estes exemplos para entender que a segurança da informação visa garantir a integridade, a confidencialidade e a autenticidade das informações processadas pela empresa. Neste contexto, confidencialidade e autenticidade significam ter certeza de que pessoas não tomem conhecimento de informações de forma acidental ou proposital e consiste na garantia de que apenas pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de qualquer compartilhamento ou rede (TRIBUNAL DE CONTAS DA UNIÃO, 2007).

Portanto, é importante que as organizações definam uma estrutura adequada para a proteção – e gestão – de suas informações, de acordo com seu porte e tipo de negócios, de modo a conscientizar todos os colaboradores de que a informação é um bem, isto é, tem valor para a empresa e deve ser protegida (FONTES, 2006).

A quebra de confidencialidade e confiança na informação são assuntos presentes em praticamente todas as organizações, sendo elas de pequeno ou grande porte onde se podem encontrar problemas não apenas com roubo de informações, como também com o vazamento ou a credibilidades das mesmas.

De acordo com Tadeu (2017), uma pesquisa divulgada por The Global State of Information Security Survey (GSISS) no último ano, empresas brasileiras sofreram uma perda decorrente de incidentes de segurança. Os prejuízos variam de acordo ao tamanho e ramo de atuação das organizações, podendo chegar entre US$ 10 mil a US$ 20 milhões ou mais. Das empresas entrevistadas, 2,2% chegaram a registrar um período de inatividade total de mais de cinco dias em razão de incidentes de

segurança. 27,7% ficaram inoperantes de três a oito horas, enquanto cerca de 20% estiveram com seus sistemas fora do ar de uma a duas horas e 17,3%, de nove a 24 horas.

Portanto, este estudo consiste em analisar problemas decorrentes com a quebra de confidencialidade dentro das organizações e propor medidas de boas práticas, focando em aspectos humanos e tecnológicos para minimizar riscos à segurança de informação dentro das organizações. Assim, auxiliando os gestores responsáveis pela segurança da informação aos problemas decorrentes de não cumprimento das regras básicas e específicas para cada elemento humano no ambiente corporativo.

1.1 PROBLEMA DE PESQUISA

Segundo Fontes (2006), a informação é a propriedade intelectual muito cobiçada pelos concorrentes, qualquer vazamento de qualquer dado sendo por descuido ou má-fé pode comprometer a participação da organização no mercado. Algumas medidas podem ser adotadas para auxiliar o controle destes dados, mas principalmente precisa-se ter comprometimento pela parte do usuário perante a confidencialidade das informações da empresa.

Grandes empresas não perdem milhões apenas em ataques sofridos por *hackers*, mas perdem muito também por conta de vazamento de informações sigilosas que os usuários da empresa deixam escapar por desleixo ou traição.

Cada dia mais as organizações estão realizando investimentos com valores altos em tecnologia e segurança, porém continuam cada vez mais vulneráveis. Necessita-se considerar vários fatores, como empregados despreparados ou mal-intencionados, ausência de políticas de segurança, normas e procedimentos pela parte da empresa, tornando-a uma porta de saída para informações sigilosas e de estratégias de mercado.

Com os inúmeros problemas de segurança que ocorrem atualmente, quais são os mecanismos e ferramentas que as organizações podem adotar para minimizar o vazamento das informações?

1.2 OBJETIVOS

O objetivo geral deste trabalho é sistematizar os principais tipos de ataque, mecanismos de segurança e ferramentas relacionados com a quebra de confidencialidade que podem ocorrer dentro de uma organização.

Tem-se como objetivos específicos:

- Identificar os principais tipos de ataque (humanos e tecnológicos) que afetam a quebra de confidencialidade dos dados no ciclo de vida da informação.
- Associar os mecanismos de segurança aos tipos de ataque no ciclo de vida da informação.
- Pesquisar ferramentas computacionais que implementem os mecanismos de segurança selecionados.
- Selecionar uma organização para verificar a sistematização elaborada e a viabilidade da implementação das ferramentas estudadas.

1.3 METODOLOGIA

Para a realização deste trabalho, será abordada uma pesquisa bibliográfica, constituído principalmente de livros, artigos de periódicos e atualmente com material disponibilizado na internet. Deste modo, visa interpretar, compreender e analisar tais dados e ações através de recursos e técnicas.

Na segunda etapa será realizado um estudo dos principais problemas de ataques humanos e tecnológicos que afetam a quebra de confidencialidade no ciclo de vida da informação.

A terceira etapa consiste em unificar quais mecanismos de segurança podem ser utilizados contra os diversos tipos de ataques no ciclo da informação e a busca de ferramentas que podem ser utilizadas na implementação dos mecanismos de segurança.

Após, será desenvolvida uma estratégia operacional. Segundo COSTA (2009), é baseado em técnicas produtivas, técnicas de comunicação e sistemas de informação.

Ainda, de acordo com Ximenes (2000), a estratégia é uma arte militar do planejamento e execução de operações relativas a pessoas e materiais, garantindo posições vantajosas para alcançar um objetivo específico.

Por estes conceitos, neste estudo, a tática se dá na preparação de um conjunto de diretrizes para o ciclo da informação da organização. Diretivas estas que levam em conta a quebra de sigilo das informações, as vulnerabilidades e as normas de segurança garantindo confidencialidade, integridade, disponibilidade e autenticidade das informações.

A quarta etapa consiste na seleção de uma organização para aplicar a estratégia operacional analisada e, após, validar e aprimorar as recomendações desenvolvidas da terceira etapa.

E por fim, a última etapa consiste na análise e avaliação dos resultados obtidos com a implementação realizada na quarta etapa do estudo de caso, a fim de sugerir melhorias nas recomendações sobre os problemas com a quebra de confidencialidade definidas.

1.4 ESTRUTURA DO TRABALHO

A estrutura deste trabalho é composta por cinco seções onde serão abordados assuntos desde definições de conceitos sobre segurança da informação, até a análise de ameaças e mecanismos de segurança que levaram ao diagnóstico de ferramentas, visando minimizar os riscos e aumentar a proteção das informações dentro das organizações. Em resumo, pode-se definir os capítulos seguintes em:

- Capítulo 2 - Segurança da Informação: É abordado conceitos de informação, princípios básicos, bem como os ciclos de vida da informação.
- Capítulo 3 - Principais ameaças, mecanismos de segurança e ferramentas: detalha as principais ameaças encontradas na literatura e mecanismos de segurança. É realizada uma análise em qual momento

do ciclo de vida da informação a ameaça ocorre e analisa quais ferramentas auxiliam na proteção destas ameaças.

- Capítulo 4 - Proposta Solução: aborda a elaboração da proposta solução para o problema apresentado no capítulo 1, bem como, análise, recomendações sobre ameaças existentes e seus mecanismos de segurança que visam minimizar os riscos.
- Capítulo 5 – Aplicação do estudo de caso na empresa XYZ, bem como as ferramentas e mecanismos de segurança que foram aplicados e seus resultados.
- Capítulo 6 – Conclusão a partir de tudo que foi estudado e desenvolvido neste documento.

2. SEGURANÇA DA INFORMAÇÃO

A informação sempre foi de grande relevância para a tomada de decisão da organização. Para Sêmola (2003), informação pode ser um conjunto de dados usados para troca de mensagens entre máquinas e pessoas. Ela pode estar presente ou pode ser manuseada por vários elementos deste processo.

Já Audy, Andrade e Cidral (2005), definem a informação como um conjunto de dados encadeados, o qual foi processado resultando em valor real ou percebido para decisões correntes e posteriores. Algumas características podem determinar seu valor para a empresa, tal como: precisa, confiável, relevante, acessível, segura, entre outras.

Na organização, conforme Fontes (2006), a informação é um ativo de grande valor e importância para a empresa. Com isso, necessita-se estar adequadamente protegida.

Segundo a norma NBR ISO/IEC 27002 (ABNT, 2013), “a segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *hardware* e *software*”. Ainda assim, esses controles precisam ser estabelecidos, implementados, monitorados, analisados e melhorados continuamente, para atender os objetivos do negócio e a segurança da informação da organização.

Ainda, Galvão (2015), afirma que a segurança da informação tem como objetivo a proteção dos sistemas contra a alteração e invasão dos dados por pessoas não autorizadas. Ela deve prevenir, detectar, deter e documentar qualquer ameaça aos seus dados e processamento, haja vista que uma informação incorreta, ou a falta dela, pode ocasionar grandes perdas que comprometam o funcionamento da organização e seu retorno (FONTES, 2006).

A segurança da informação pode ser classificada em técnicas, conceitos, procedimentos e mapeamentos que gerenciam as informações de modo a desenvolver um planejamento estratégico para garantir a proteção das informações.

Entre esses métodos, três deles devem ganhar importância quando se trata de prevenção da informação: confiabilidade, integridade e disponibilidade.

2.1 PRINCÍPIOS BÁSICOS DA INFORMAÇÃO

A tríade conhecida por CIA (*Confidentiality, Integrity and Availability*) representam os princípios básicos da segurança da informação, demonstrado na Figura 1.

Figura 1 - Segurança da Informação - Tríade CIA

Fonte: ABREU (2011).

De acordo com Fontes (2006), a informação apenas deve ser utilizada e acessada exclusivamente por quem necessita da informação e por quem tem permissão de acesso e uso dentro das organizações. Para Galvão (2015), confidencialidade representa a garantia que a informação estará acessível somente para a pessoa autorizada. Se uma pessoa sem autorização tem conhecimento, ocorre uma violação de privacidade.

Dito de outra forma, privacidade está relacionada com a propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

A integridade refere-se à indicação inequívoca de que as mensagens transmitidas entre emissor e receptor não tenham sido adulteradas acidentalmente ou por terceiros ao longo do trajeto entre estes nós.

Logo, Palma (2016) diz que, a integridade é um pilar essencial para os processos de negócio, onde informações corrompidas geram grandes problemas, ou também, necessidade de correção e retrabalho quando tratadas em tempo.

Já para Galvão (2015), a integridade visa garantir que as informações armazenadas estejam corretas, verdadeiras e não sofreram nenhum tipo de alteração e violação. É a garantia de que os dados armazenados coincidem com os incluídos.

A disponibilidade é a garantia de que os usuários autorizados tenham acesso a informações e ativos associados quando necessário. De acordo com Galvão (2015), disponibilidade é a garantia de que, quando as pessoas autorizadas solicitarem alguma informação, estas estejam disponíveis.

De outra forma, é a propriedade da informação estar acessível e utilizável quando solicitada por uma pessoa autorizada.

2.2 CONCEITOS RELACIONADOS À SEGURANÇA DA INFORMAÇÃO

Para entender melhor a segurança da informação é necessário primeiramente entender alguns conceitos básicos como: ameaças, vulnerabilidades, ativos, ataques, mecanismos de segurança e ciclo de vida da informação.

Pode-se entender por **ameaça** todo e qualquer fator que pode causar algum incidente ou problema que possa prejudicar a organização de alguma forma. (GALVÃO, 2015).

Conforme Sêmola (2003), as ameaças são agentes ou condições que afetam as informações e seus ativos, explorando as vulnerabilidades, gerando incidentes de perda de confidencialidade e impactos aos negócios da empresa.

Vulnerabilidade é definida como uma falha no projeto, implementação ou configuração de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

De acordo com Galvão (2015), fraqueza e fragilidade estão relacionados ao ativo da empresa e podem ser compreendidos como vulnerabilidade na estrutura organizacional, facilitando uma ameaça, causando um incidente.

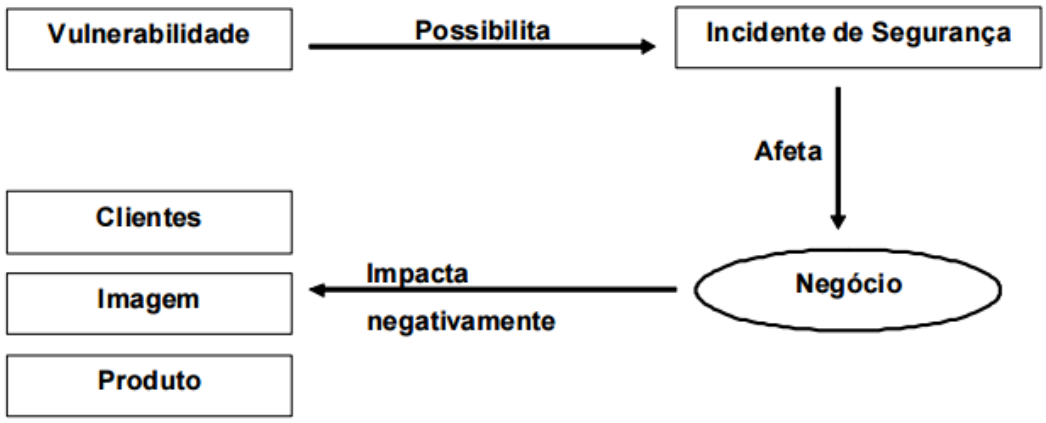
Sêmola (2003), afirma que vulnerabilidades são fragilidades presentes ou associadas a ativos que manipulam e/ou processam dados. Elas não provocam incidentes, por serem dados passivos, necessitando de um agente causador ou condição favorável, vazamento ou incêndio.

Alguns exemplos de vulnerabilidades podem ser classificados em:

- Elementos físicos: como salas mal planejadas, falta de extintores, detectores de fumaça e outros recursos para combater incêndios e riscos de explosões.
- Naturais: como os computadores são suscetíveis a desastres naturais, como incêndios, enchentes, terremotos.
- *Hardware*: falha de recursos tecnológicos ou erros durante a instalação.
- *Software*: erros de instalações ou configurações podem acarretar acessos indevidos, vazamentos das informações, perda dos dados ou indisponibilidade. Mídias como discos, mídias, fitas podem ser perdidos ou danificados. Comunicação, como acessos não autorizados ou perda de comunicação.
- Elementos humanos: como a falta de treinamento, compartilhamento das informações confidenciais, sabotagens, greves, invasões.

A vulnerabilidade pode levar à ocorrência de determinados incidentes de segurança, sendo assim elas são as principais causas das falhas de segurança (Figura 2).

Figura 2 - Vulnerabilidade



Fonte: LAUREANO (2005).

A Figura 2 mostra que a vulnerabilidade tem relação direta com os negócios da organização, afetando seus ativos, e impactando negativamente o vínculo com os clientes, imagem da companhia e seus produtos.

Ativos são elementos que fazem parte dos processos de manipulação e processamento da informação. Podem ser definidos como ativos: a própria informação, meio que é armazenada, pessoa, tecnologia, sistemas, equipamentos utilizados para manuseá-la, transportá-la, descartá-la e que possua valor.

Em concordância com Sêmola (2003), ativo é tudo que compõe os processos que manipulam e processam as informações, sua informação, o meio em que ela é armazenada, onde ela é manuseada, transportada e descartada.

Para Galvão (2015), ativo significa qualquer parte que componha a organização, sendo ela, uma pessoa, sistema, tecnologia e todos que são ou não responsáveis por um processo ou por uma área específica da empresa.

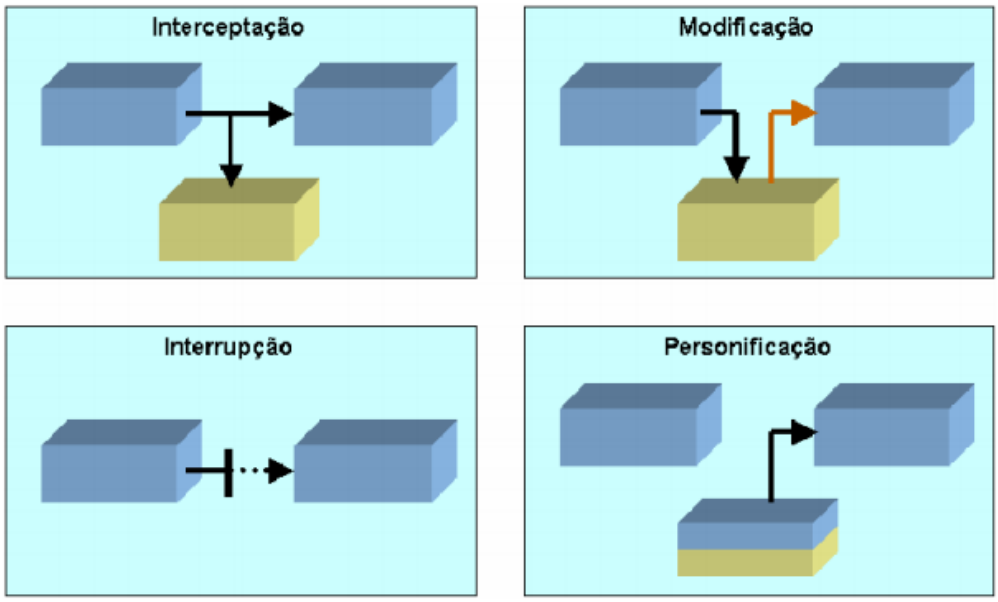
Os **ataques** podem ser definidos como um problema de segurança, tal que, um agente busca obter algum tipo de retorno, atingindo um ativo de valor. Seu retorno pode ser financeiro ou não (ALBURQUERQUE; RIBEIRO, 2002).

De acordo com Oliveira (2001), o ataque é a coleta dos dados e informações sobre seu alvo. O atacante tentará o máximo de informações sobre seu alvo.

O fato de um sistema estar sendo atacado, não significa que seus dados serão afetados. Segundo Laureano (2005), um ataque só terá sucesso dependendo da vulnerabilidade do sistema e das medidas de proteção que ele possui.

Podem ser classificados como formas de ataques: Vírus, *Trojans* ou Cavalo de Tróia, *Worms*, Engenharia social entre outros. Quando um ataque ocorre, o fluxo normal de transmissão dos dados é alterado. Este fluxo normal pode ser alterado por mecanismos de ataques, bem como: interrupção, interceptação, modificação e personificação (Figura 3).

Figura 3 - Tipos de Ataques



Fonte: LAUREANO (2005).

Para Laureano (2015), interrupção é quando a informação ficará indisponível, não é mais possível acessá-la, interrompendo o fluxo normal da mensagem ao destino. Interceptação é quando informações sigilosas poderão ser visualizadas por pessoas sem autorização. Modificação incide na alteração das informações por pessoas não autorizadas, violação da integridade da mensagem. Personificação define-se como uma pessoa que acessa as informações ou a transmite se passando por pessoas autênticas, violação da autenticidade.

Para Sêmola (2003), os **mecanismos de segurança** da informação são práticas, procedimentos e mecanismos usados para a proteção das informações e

seus ativos, prevenindo contra as ameaças e impedindo que estas explorem vulnerabilidades.

Algumas medidas de segurança são consideradas controles que podem ter as seguintes características: preventivas, detectáveis e corretivas.

Medidas preventivas, segundo Sêmola (2003), são medidas cujo objetivo são evitar incidentes que possam acontecer. Visam manter a segurança já implementada que estabeleçam a conduta e a ética da segurança da organização. Como exemplos, podem-se citar as políticas de segurança, procedimentos e normas, palestras de conscientização de usuários, ferramentas como *firewall* e antivírus.

Medidas detectáveis são medidas que visam identificar condições ou indivíduos causadores de ameaças, a fim de evitar que as ameaças explorem vulnerabilidades. Pode-se citar como exemplos, a análise de risco, IDS *(Intrusion Detection System)*, câmeras de vigilância e alarmes.

Medidas corretivas são ações voltadas à correção de uma estrutura tecnológica e humana, para que se adaptem às condições de segurança estabelecidas pela organização ou voltadas à redução dos impactos. Exemplos de medidas corretivas são *backups*, plano de continuidade operacional e plano de recuperação de desastres.

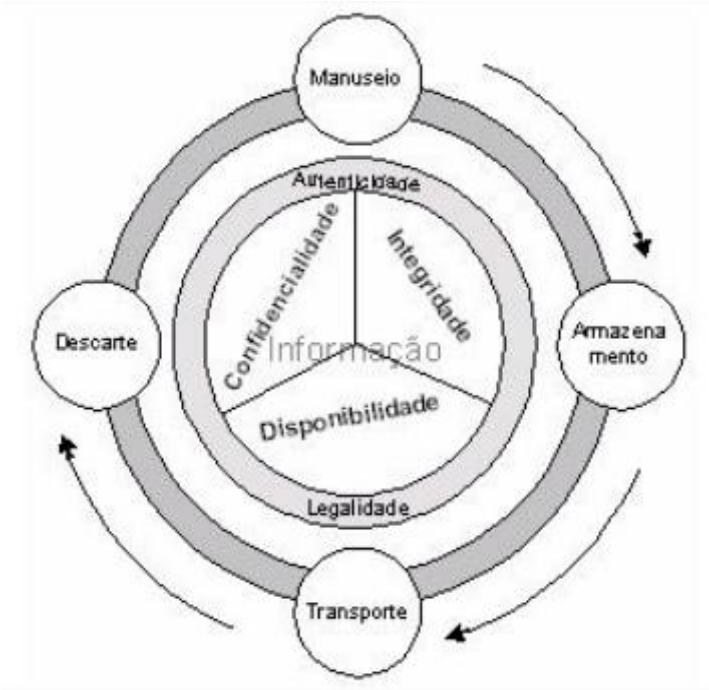
Os mecanismos de segurança da informação envolvem controles físicos e lógicos referentes ao *software*, *hardware* e também humanos.

De acordo com Santana (2013), controles físicos definem-se como um conjunto de medidas capaz de controlar acesso das pessoas. Realizado por restrições de acesso e registro que servem como barreira adicional ao acesso lógico. Alguns exemplos de controles físicos são: portas blindadas, detectores de metal, catracas com leitura biométrica, fechaduras com senhas. Controles lógicos podem ser definidos como barreiras que impedem ou limitam acesso à informação em meio eletrônico, tal como, criptografia, assinatura digital, tipos de autenticação, firewalls e autenticação.

2.3 CICLO DE VIDA DA INFORMAÇÃO

O ciclo de vida da informação, segundo Sêmola (2003), é composto e identificado pelos momentos em que a informação é colocada em risco, onde compõem e identificam o ciclo de vida da informação. As fases que compõem o ciclo de vida da informação (Figura 4) são:

Figura 4 - Quatro momentos do ciclo de vida da informação



Fonte: SÊMOLA (2003).

- **Manuseio:** abrange a criação ou alteração da informação.
- **Armazenamento**: quando a informação é armazenada, por exemplo, em um banco de dados, anotações no papel ou arquivo digital.
- **Transporte**: momento em que a informação é conduzida ou transportada, seja ela por meio eletrônico ou fax.
- **Descarte**: é o momento quando a informação é descartada, excluída ou inutilizada, como por exemplo, quando um registro, arquivo eletrônico ou papel é excluído.

De acordo com Galvão (2015), em cada etapa do ciclo da informação é necessário garantir confidencialidade, integridade, autenticidade, disponibilidade e também legalidade aos dados de maneira eficaz.

2.4 CONSIDERAÇÕES FINAIS

A segurança da informação mostra-se como um item fundamental na proteção dos ativos de um usuário ou organização. Estruturada por pilares chave como confidencialidade, integridade e disponibilidade, a informação demanda mecanismos de segurança, sejam físicos ou lógicos, que reduzam a vulnerabilidade dos sistemas e inibam eventuais ataques aos dados. Mais do que isso, devem garantir um ciclo de vida seguro da informação, desde sua criação até o seu descarte.

Em tempo, destaca-se a importância destes conceitos como alicerce aos temas que envolvem a segurança da informação. Estes conceitos aplicados devem prever os diversos tipos de ataques e frustrar a quebra de confidencialidade da informação.

Após conhecer conceitos básicos da segurança da informação e algumas normas relacionadas a eles, o próximo passo é identificar as principais ameaças e mecanismos de segurança que existem atualmente. Este assunto é abordado no Capítulo 3.

3. PRINCIPAIS AMEAÇAS, MECANISMOS DE SEGURANÇA E FERRAMENTAS

A informação é um dos ativos mais valiosos de uma organização. A informação, como os outros ativos relacionados com ela, deve ser adequadamente protegida independentemente da forma como são tratadas, processados, transportados, armazenados ou eliminados. A segurança da informação inclui todos os processos de informação, físicos e eletrônicos, independentemente de eles envolverem pessoas, tecnologia ou as relações com os parceiros comerciais, clientes e terceiros.

Este capítulo apresenta um levantamento das principais ameaças e mecanismos de segurança da informação (seções 3.1 e 3.2) e algumas ferramentas que podem ser utilizadas para proteger a informação (seção 3.3).

3.1 AMEAÇAS

Ameaças são quaisquer eventos que explorem vulnerabilidades, com potencial de causar incidentes indesejados, resultando em danos para a organização. As ameaças podem afetar mais de um ativo, provocando impactos que variam de acordo com o tipo e a importância do ativo (ABNT NBR ISO/IEC 27005, 2011). As principais ameaças encontradas na literatura (OLIVEIRA, 2001; ABNT NBR ISO/IEC 27005, 2011; SÊMOLA, 2003; STALLINGS, 2008) são descritas no Quadro 1.

Quadro 1 - Ameaças

(continua)

Tipos de Ameaça	Definição
Processamento Ilegal dos Dados	A informação sofre uma série de tarefas sequencialmente realizadas com o intuito de produzir um arranjo determinado de informações a partir de outras obtidas inicialmente sem autorização.
Divulgação Indevida	A informação é processada e divulgada sem autorização do proprietário.
Cópia Ilegal	A informação é processada e copiada outro local sem permissão.

(continuação)

Espionagem Interna e Externa	Ato ou efeito de espionar, podendo ser de pessoas de fora ou de dentro da empresa.
Dano físico à mídia	Quando o dispositivo ou mídia sofre alguma ação de prejuízo, acidental ou intencionalmente ocasionando a perda dos dados e da mídia.
Engenharia Social	Manipulação psicológica de pessoas para a execução de ações ou divulgação das informações confidenciais.
Modificação de dados sem autorização	A informação é alterada/modificada sem autorização do proprietário.
Ataques baseados em senhas	Um *software* malicioso realiza a execução de algoritmos baseados em dicionários de palavras na tentativa de descobrir a senha original.
Acesso não autorizado das informações	A informação é acessada por pessoas sem permissão.
Abuso de poder	Membro da organização com posição hierárquica maior utiliza-se de sua autoridade para obter acesso às informações sigilosas.
Espionagem à distância	Ato ou efeito de espionar.
Comprometimento dos dados	A informação sofre algum incidente de tal forma que perca sua integridade.
Acesso a links de fontes não conhecidas ou não confiáveis	Sítios são acessados sem conhecimento da sua origem.
Furto de equipamentos	Roubo dos equipamentos da organização tornando as informações dos dispositivos inacessíveis.
Defeito de *Software*	O serviço prestado pelo *software* é desviado do serviço correto.
Falha de Equipamento	Um equipamento (*hardware*) apresenta problemas de funcionamento.
Uso não autorizado do equipamento	O equipamento é utilizado por pessoas sem autorização.
Falhas de protocolo	Alguma falha de comunicação entre os protocolos, deixando vulnerável a interceptação da informação.
Acesso a informações de fontes não confiáveis	Dados são acessados sem conhecimento da sua origem.
Exploração de vulnerabilidade	Falhas de processos que quando exploradas resulta na violação da segurança das informações.
Falhas de Autenticação	O sistema possui erros de projetos levando a falhas de autenticação.
Cópia não autorizada dos dados	A informação é processada e copiada a outro local sem permissão.
Software Malicioso	*Software* indesejado instalado sem consentimento deixando as informações vulneráveis.
DDoS / DOS- Ataques de Negação de Serviço	Ataques que visam causar indisponibilidade dos serviços de um determinado processo através do envio de simultâneas requisições.

Fonte: Próprio autor.

A maioria das ameaças podem causar incidentes de segurança em todas as etapas do ciclo de vida da informação: criação, armazenamento, transporte e descarte. Por exemplo, um ataque de força bruta pode ocorrer e gerar problemas de segurança no momento em que a informação está sendo criada, armazenada, transportada ou descartada.

Algumas ameaças podem não ser comuns de ocorrerem em todas as etapas do ciclo de vida.

A espionagem à distância e o acesso de links de fontes não conhecidas ou não confiáveis geralmente não afetam a criação e nem o descarte da informação pois a ameaça ocorre somente quando o arquivo/dado já está ativo, incidindo o risco apenas no armazenamento e transporte.

Ameaças como dano físico à mídia, furto dos equipamentos, defeito de equipamentos, modificação ilegal dos dados não ocorrem no momento do descarte da informação pois se os equipamentos/informações não forem mais úteis para o negócio, dificilmente poderá afetar o negócio da empresa.

Em paralelo, algumas ameaças se fazem presente na fase do descarte, sendo assim, se uma informação for descartada incorretamente, a mesma poderá ser utilizada ilegalmente por pessoas mal-intencionadas, tornar-se um problema para os negócios da organização.

O Quadro 2 relaciona cada uma das principais ameaças apresentadas no Quadro 1 com o momento (criação, armazenamento, transporte e descarte) que elas podem ocorrer no ciclo de vida da informação.

Quadro 2 - Ameaça - Ciclo de Vida da Informação

(continua)

Ameaça	**Criação**	**Armazenamento**	**Transporte**	**Descarte**
Processamento ilegal dos dados	X	X	X	X
Acesso não autorizado das informações	X	X	X	X

(conclusão)

Dano físico à mídia	X	X	X	
Furto dos Equipamentos	X	X	X	
Defeito de Equipamentos	X	X	X	
Modificação ilegal dos dados	X	X	X	
Acesso não autorizado aos equipamentos	X		X	X
Ataques baseados em senhas	X	X	X	X
Força bruta	X	X	X	X
Divulgação indevida das informações	X	X	X	X
Cópia ilegal dos dados	X	X	X	X
Espionagem interna	X	X	X	X
Espionagem à distância		X	X	
Software malicioso	X	X	X	
Destruição de arquivos	X	X	X	
Defeito de *software*	X	X	X	
Acesso de links de fontes não conhecidas ou não confiáveis		X	X	
Falhas de protocolos	X	X	X	
Ataques à rede de computadores	X	X	X	
Destruição de Equipamentos		X	X	X

Fonte: Próprio autor.

3.2 MECANISMOS DE SEGURANÇA

Conforme já foi mencionado no capítulo 2, os mecanismos de segurança são técnicas e/ou métodos que tentam limitar o acesso à informação, reduzindo o risco da ocorrência de crimes digitais e cibernéticos, consequentemente protegendo os ativos da organização. Os principais mecanismos de segurança encontrados na literatura (INTECO, 2010; OLIVEIRA, 2001; STALLINGS, 2003; MACÊDO, 2014; SÊMOLA, 2003) são descritos no Quadro 3.

Quadro 3 - Mecanismos de Segurança

(continua)

	Mecanismos de Segurança	**Referência**
Tráfego de rede	Virtual Private Network (VPN)	É uma aplicação de criptografia entre dois pontos distintos através de uma rede pública ou de propriedade de terceiros (SÊMOLA, 2003).
	Security Socket Layer (SSL)	Protocolo executável em servidores web e nos *browsers*, garantindo, por meio de criptografia, o tráfego dos dados na internet (OLIVEIRA, 2001).

(continuação)

Tráfego de rede	IPv6	Protocolo de comunicação de dados que possibilita a utilização de autenticação e criptografia dos dados.
	Controle de tráfego de rede	Observar as políticas de segurança da informação e permite controlar o tráfego das informações da rede (INTECO, 2010).
	SET	Protocolo semelhante ao SSL, porém voltado para transações comerciais (OLIVEIRA, 2001).
Acesso Lógico	Firewall	É uma barreira entre a rede local e a internet através da qual só passa tráfego autorizado (INTECO, 2010; OLIVEIRA, 2001).
	Proxy Systems	Implementações na interação entre cliente e servidor que visam prover apenas as facilidades necessárias para fornecer o serviço (OLIVEIRA, 2001).
	Detector de Intrusos	Dispositivo complementar ao *firewall* agregando inteligência ao processo de combate a ataques e invasões (SÊMOLA, 2003).
	Autenticação	Ato de confirmar que algo ou alguém é autêntico, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeiro (ABREU, 2011).
	Antivírus	É uma ferramenta que é utilizada para a proteção do computador, onde ele detecta e elimina os vírus (STALLINGS, 2003).
	Anti-malware	Ferramentas destinadas à proteção de sistemas contra qualquer tipo de *software* malicioso (INTECO, 2010).
Codificação	Sistemas de Antifraude	Protegem usuários e informações de abusos como roubo de informações pessoais (INTECO, 2010).
	Criptografia	Transformar uma mensagem em outra com a elaboração de um algoritmo com funções matemáticas e uma senha especial, chamada chave (OLIVEIRA, 2001).
	Esteganografia[1]	Propõe o uso de métodos de camuflagem de informações sigilosas em mensagens e arquivos aparentemente inofensivos, que só poderiam ser extraídas pelo destinatário (SÊMOLA, 2003; MATTOS, 2005).
	Sistemas e ferramentas de criptografia	Ferramentas que auxiliam na proteção a confidencialidade das informações no transporte e no armazenamento, permitindo a criptografia dos dados (INTECO, 2010).

[1] Esteganografia é uma técnica voltada à privacidade no envio de informações. Ela utiliza métodos de camuflagem de informações sigilosas em mensagens e arquivos aparentemente inofensivos, o qual só pode ser extraído pelo destinatário que detém do conhecimento do mapa de camuflagem.

(conclusão)

Codifi-cação	Autenticação Digital e certificação	Produtos destinados ao uso e utilização de certificados digitais fornecendo mais segurança aos processos, aplicações e sistemas (INTECO, 2010).
Físicos	Dispositivos de proteção física de equipamentos	Equipamentos utilizados para a proteção de seus ativos contra furto (INTECO, 2010).
Backups	Cópias de Segurança	Cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso de perda dos dados originais (MACÊDO, 2014).
Gerencial	Plano de continuidade[2]	Ferramentas que facilitam e permitem o gerenciamento de planos de contingência e continuidade, realizando melhoria contínua e gerenciamento dos incidentes (INTECO, 2010).
	Acesso e identificação da gestão de controle	Ferramentas que evitam a difusão e vazamento sendo acidental ou deliberada das informações ou dados fora da organização (INTECO, 2010).
	Termo de Responsabilidade e confidencialidade	Tem o propósito de formalizar o compromisso e o entendimento do funcionário diante de suas novas responsabilidades relacionadas à proteção das informações que manipula (SÊMOLA, 2003).

Fonte: Próprio autor

Após o estudo destes mecanismos, unificou-se eles entre grupos de semelhanças e funcionalidades e foi relacionado eles com suas ameaças em seus ciclos de vida. Os mecanismos de controle de tráfego de rede, VPN, SSL e IPv6 utilizam mecanismos de criptografia e autenticação e protegem os dados enquanto eles trafegam nas redes de computadores. Esses mecanismos podem auxiliar a evitar ameaças como o processamento ilegal dos dados, o acesso não autorizado às informações, a modificação ilegal dos dados, a divulgação indevida das informações, a cópia ilegal dos dados, a espionagem interna e a espionagem à distância entre outros conforme apresentado no Quadro 4.

[2] Plano de continuidade engloba plano de contingência (para situações onde ocorram perdas de recursos, mas estes podem ser recuperados), plano para recuperação de desastre (para situações onde ocorram perdas/rupturas de recursos, mas a recuperação exige esforço) e plano de emergência (não existe perda no recurso, mas sofrimento de recursos).

Quadro 4 – Tráfego de Rede

Categoria do Mecanismo de Segurança	Ameaça	Criação	Armazenamento	Transporte	Descarte
Tráfego de Rede	Processamento ilegal dos dados	X	X	X	X
	Acesso não autorizado das informações	X	X	X	X
	Modificação ilegal dos dados	X	X	X	
	Divulgação indevida das informações	X	X	X	X
	Cópia ilegal dos dados	X	X	X	X
	Espionagem interna	X	X	X	X
	Espionagem à distância		X	X	
	Acesso de links de fontes não conhecidas ou não confiáveis		X	X	
	Falhas de protocolos	X	X	X	
	Ataques à rede de computadores	X	X	X	

Fonte: Próprio autor

O grupo de acesso lógico cujo objetivo é a verificação da identidade e autenticidade dos usuários e a proteção dos dados, programas e sistemas contra tentativas de acesso não autorizado.

As ameaças deste grupo estão ligadas com o processamento, acesso, modificação ilegal dos dados, ataques à rede de computadores e também no furto e acesso não autorizado aos equipamentos. O Quadro 5 sintetiza todas as possíveis ameaças levantadas deste grupo.

Quadro 5 – Acesso Lógico

(continua)

Categoria do Mecanismo de Segurança	Ameaça	Criação	Armazenamento	Transporte	Descarte
Acesso Lógico	Processamento ilegal dos dados	X	X	X	X
	Acesso não autorizado das informações	X	X	X	X
	Furto dos Equipamentos	X	X	X	
	Modificação ilegal dos dados	X	X	X	X
	Acesso não autorizado aos equipamentos	X		X	X

(conclusão)

Acesso Lógico	Ataques baseados em senhas	X	X	X	X
	Força bruta	X	X	X	X
	Espionagem à distância		X	X	
	Software malicioso	X	X	X	
	Destruição de arquivos	X	X		
	Acesso de links de fontes não conhecidas ou não confiáveis		X	X	
	Ataques à rede de computadores	X	X	X	

Fonte: Próprio autor

No grupo determinado codificação, baseado em sistemas de antifraude, sistemas e ferramentas de criptografia, esteganografia, e certificados digitais são responsáveis pela codificação e camuflagem dos dados originais, na tentativa de converter a informação original e direcionar a leitura apenas para o destinatário.

Esta codificação defende no processamento ilegal dos dados, acesso não autorizado das informações e na modificação ilegal dos dados. No quadro 6 - Codificação resume estas ameaças deste grupo.

Quadro 6 – Codificação

Categoria do Mecanismo de Segurança	**Ameaça**	**Criação**	**Armazenamento**	**Transporte**	**Descarte**
Codificação	Processamento ilegal dos dados	X	X	X	X
	Acesso não autorizado das informações	X	X	X	X
	Modificação ilegal dos dados	X	X	X	X

Fonte: Próprio autor

O grupo físico, que é responsável pela proteção física dos equipamentos é encontrado a ameaça de falha de equipamentos, referindo-se quando um equipamento, geralmente *hardware*, apresenta problemas de mau funcionamento conforme Quadro 7 - Físico.

Quadro 7 - Físico

Categoria do Mecanismo de Segurança	Ameaça	Criação	Armazenamento	Transporte	Descarte
Físico	Falha de Equipamentos		X	X	X

Fonte: Próprio autor

O grupo backups é responsável pelas cópias de segurança, a existência de cópia de um ou mais arquivos guardados em diferentes dispositivos de armazenamento. Se, por qualquer motivo, houver perda dos arquivos originais, a cópia de segurança armazenada pode ser restaurada para repor os dados perdidos. O backup protege os dados contra as ameaças do dano físico a mídia, furto e defeito/falhas de equipamentos, conforme Quadro 8 – Backups.

Quadro 8 – Backups

Categoria do Mecanismo de Segurança	Ameaça	Criação	Armazenamento	Transporte	Descarte
Backups	Dano físico à mídia	X	X	X	
	Furto dos Equipamentos	X		X	
	Defeito de Equipamentos	X	X		

Fonte: Próprio autor

Os mecanismos gerenciais estão diretamente ligados ao plano de continuidade, gestão da identidade e termo de responsabilidade e confidencialidade. Este grupo refere-se a um conjunto de estratégias e planos de ação preventivos que garantem o pleno funcionamento dos serviços essenciais de uma empresa durante quaisquer tipos de falhas, até que a situação seja normalizada. Em paralelo também é responsável pela gestão de acessos e repasse das novas responsabilidades relacionadas à proteção das informações que cada colaborador manipula diariamente.

As ameaças deste grupo são encontradas no processamento, acesso, modificação, cópia ilegal dos dados, furto, defeito de equipamentos, divulgação indevida, *software* malicioso, falhas de protocolo entre outras. O Quadro 9 – Gerencial resume as ameaças levantadas.

Quadro 9 – Gerencial

Categoria do Mecanismo de Segurança	**Ameaça**	**Criação**	**Armazenamento**	**Transporte**	**Descarte**
Gerencial	Processamento ilegal dos dados	X	X	X	X
	Acesso não autorizado das informações		X	X	
	Furto dos Equipamentos		X	X	
	Defeito de Equipamentos		X	X	
	Modificação ilegal dos dados	X	X	X	
	Divulgação indevida das informações	X	X	X	X
	Cópia ilegal dos dados	X	X	X	X
	Espionagem interna	X	X	X	X
	Software malicioso	X	X	X	
	Defeito de *software*	X	X	X	
	Acesso de links de fontes não conhecidas ou não confiáveis		X	X	
	Falhas de protocolos	X	X	X	
	Ataques à rede de computadores	X	X	X	
	Destruição de Equipamentos		X	X	X

Fonte: Próprio autor

Visando a busca por uma forma mais simplificada de entender a relação entre mecanismos e ferramentas, realizou-se o levantamento e a análise das possíveis ameaças encontradas na literatura sobre a quebra do sigilo da informação dentro das organizações. Considera-se também mecanismos de segurança para auxiliar na redução ou eliminação destas ameaças, limitando o contato ou acesso direto à informação no meio eletrônico e também físico das informações e equipamentos. Em paralelo, foram relacionadas as ameaças com seu ciclo de vida da informação, isto é, analisado em que momento no ciclo de vida a informação pode sofrer tais ameaças.

Em síntese, ficou claro que a informação está vulnerável em praticamente todo o ciclo da informação. Para auxiliar na proteção destes dados, realizou-se o levantamento de mecanismos de segurança para cada ameaça encontrada.

Este levantamento é classificado como exploratório, ou seja, após levantamento bibliográfico, buscou-se sobre ferramentas com conceitos elevados no mercado nos últimos dois anos de acordo com alguns sites que realizam pesquisas sobre melhores *softwares*[3].

A seguir, tem-se uma relação de ferramentas encontradas no mercado, algumas gratuitas, outras pagas e algumas *OpenSource* (código aberto) que ajudam a proteger de tais ameaças. Estas ferramentas dão suporte a praticamente todos os sistemas operacionais (Windows, Linux, MAC OS), algumas fornecem suporte também para smartphones e tablets com sistemas operacionais Android e iOs. Informações detalhadas sobre estas ferramentas encontram-se no Apêndice A.

Quadro 10 – Ferramentas

(continua)

Mecanismo de Segurança	**Ferramenta**
Firewall	ZoneAlarm Firewall Comodo Internet Security Iptables
Controle de tráfego de rede	NLoad GFI LanGuard Wireshark
Sistema e ferramentas de criptografia	Comodo Disk Encryption Steganos Safe VeraCrypt
Autenticação	Certificados Digitais - CEF Tokens Identificadores Biométricos
Cópias de Segurança	Advanced Maryland Automatic Network Disk Archiver - AMANDA Acronis True Image NovaBackup
Anti-Malware	Malwarebytes IOBit Malware Fighter ClamAV para Linux
Esteganografia	Image Steganography Steghide
Antivírus	McAfee Norton Panda

[3] Site Top Ten (top10mais.org/), TechTudo (www.techtudo.com.br) e Topfreeware (http://www.topfreewares.com.br).

(conclusão)

Virtual Private Network	ExpressVPN NordVPN PureVPN
Sistemas de detecção de intrusão (IDS)	SNORT *OSSEC-HIDS*
Gestão de Identidade	Gerenciamento de identidade e acesso Oracle Gestão de identidades e acessos - Microsoft
Dispositivos de proteção física de equipamentos	Cabo de Aço - Antifurto

Fonte: Próprio autor.

As ferramentas que estão associadas mais diretamente com a confidencialidade dos dados são aquelas que fornecem criptografia. Algumas delas, tal como Comodo Disk Encryption, Steganos Safe e VeraCrypt auxiliam na proteção do disco rígido através de criptografia, restringindo o uso de arquivos apenas ao administrador de acordo com suas configurações. Estas ferramentas utilizam algoritmos fortes para garantir sigilo no acesso e afastar usuários maliciosos. Outras ferramentas que aplicam métodos de criptografia semelhantes são os mecanismos que utilizam autenticação. Encontrados atualmente nos tokens de bancos, certificados digitais e identificadores biométricos.

Em paralelo, encontram-se outras ferramentas com conceitos semelhantes à criptografia além da autenticação. A esteganografia compreende de técnicas que permitem esconder informações dentro de outros arquivos, camuflando os dados como textos inteiros, músicas, vídeos ou documentos. Entre criptografia e esteganografia existe uma diferença, a criptografia oculta o significado da mensagem e a esteganografia oculta à existência da mensagem. Ambas têm como objetivo assegurar que a informação chegue ao seu destino sem ser acessada ou violada.

Mas não é só a criptografia que auxilia na proteção da confidencialidade dos dados. No firewall, por exemplo, foram encontradas várias ferramentas gratuitas e pagas, porém citadas apenas três. Firewall pode ser definido como um conjunto de componentes que monitoram o tráfego de rede de entrada e saída conforme o conjunto definido de regras de segurança. Ele protege não só a integridade dos dados na rede, mas também a confidencialidade deles, limitando o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

Os antivírus pesquisados, tal como, McAfee, Norton e Panda, são ferramentas que, previamente configuradas, detectam, impedem e atuam na remoção de programas de *software* maliciosos, como vírus e *worms* protegendo as informações de serem contagiadas ou raptadas. Esta ação garante a integridade dos dados haja vista que o risco de acesso indevido à informação é minimizado pela proteção do antivírus, o que contribui para a confidencialidade dos dados.

Em paralelo, é possível encontrar outras ferramentas semelhantes ao antivírus que auxiliam na remoção avançada de pragas digitais chamadas de anti-*malware*.

Conforme estudado neste capítulo, os principais mecanismos de segurança e ameaças são possíveis encontrar diversas ferramentas de segurança disponíveis no mercado para auxiliar no controle e na redução das ameaças em relação à quebra de confidencialidade da informação. O próximo capítulo fará a descrição da proposta solução deste trabalho.

4. PROPOSTA SOLUÇÃO

A proposta de solução do trabalho consiste na seleção de uma empresa de pequeno porte, a análise do seu cenário, o levantamento de ameaças que podem ocorrer no ciclo de vida da informação e a definição e teste de ferramentas que podem auxiliar na prevenção de ataques através da elaboração de uma estratégia operacional.

A estratégia operacional, conforme referenciada na metodologia do capítulo 1, incide em organizar e planejar as etapas de execução do estudo de caso, desde a identificação das ameaças até a implementação e acompanhamento das melhorias, visando alcançar os objetivos em sua totalidade.

Neste contexto, entende-se a necessidade de uma ordem cronológica e estrategicamente disposta de atividades. São elas:

1. Aplicação prévia de um questionário quanto à segurança da informação na organização.
2. Análise dos objetivos protecionistas da organização.
3. Análise dos aspectos econômicos da organização.
4. Levantamento dos Mecanismos de Segurança cabíveis à correção do(s) risco(s).
5. Levantamento das ferramentas viáveis para aplicação.
6. Aplicação prática das Ferramentas.
7. Aplicação final do questionário.
8. Avaliação dos resultados.

Aplica-se com antecipação um questionário com objetivo de diagnosticar a maturidade da empresa quanto ao zelo de suas informações. Serão considerados o entendimento e a preocupação que a organização tem em relação à segurança da informação, ameaças e se ela já utiliza alguma ferramenta referente à quebra de confidencialidade.

Após, será iniciada a análise de riscos dentro da organização. Este processo contempla a definição do contexto, identificação das ameaças, vulnerabilidades, ativos, controles inexistentes, consequências, estimativas dos riscos, os impactos e os tipos de tratamento, tomando por base o status no ciclo de vida da informação, bem como, os aspectos humanos, tecnológicos ou físicos.

Neste momento, levam-se em conta as respostas do questionário buscando falhas operacionais na organização. Nesta etapa também serão analisados os riscos em cima de algum processo importante da empresa que esteja com deficiência, medindo o que acontece com a informação no ciclo de vida dela e usando como parâmetro as ameaças e os mecanismos estudados no capítulo 3.

No terceiro e quarto passo, avalia-se junto ao plano diretor se a empresa tem como objetivo assegurar a confidencialidade de seus dados e suas informações como fundamentos da segurança e perpetuação de negócio. Também serão ponderadas questões orçamentárias e riscos calculados quanto à segurança da informação bem como a viabilidade financeira e temporária da organização.

Uma vez identificadas as ameaças, relaciona-se os mecanismos de segurança que poderão atuar no sentido de minimizar a ocorrência das ameaças levando em consideração as particularidades da empresa.

Alinhados os objetivos da organização quanto às ameaças encontradas, iniciará o processo de análise de mecanismos de segurança e ferramentas para aplicação. Os mecanismos de segurança serão selecionados de acordo com a deficiência levantada e, após, serão avaliadas as ferramentas cabíveis para minimizar os riscos encontrados conforme o terceiro e quarto passos.

Na seleção das ferramentas, as ameaças serão analisadas e cruzadas com a importância que a empresa determina às suas informações. Esta classificação será dividida em dois grupos: críticos e intermediários. As ameaças que forem analisadas com baixo risco para a empresa ou se, mesmo ocorrendo o incidente a empresa não será afetada de nenhuma maneira, não serão tratadas com a aplicação de ferramentas.

As ameaças avaliadas como intermediárias ou críticas serão classificadas em grau de importância após análise técnica e serão definidas ferramentas de acordo

com seus níveis, isto é, se há necessidade de realizar investimentos em ferramentas ou se o mercado oferece ferramentas com as mesmas funcionalidades ou que suprem a necessidade de forma gratuita.

Após a definição das ferramentas, será alinhado junto à empresa como será realizada a implantação das ferramentas e mudanças de hábitos que possam ocorrer neste período do estudo de caso.

Após a implantação, será aplicado novamente o questionário a fim de realizar comparativos com o primeiro questionário avaliando a evolução do pensamento e amadurecimento quanto à segurança da informação. Por fim, avalia-se a efetividade da ferramenta na contenção das ameaças anteriormente elencadas.

4.1 QUESTIONÁRIO DE PESQUISA

De acordo com Dresch, Lacerda e Júnior (2015), o questionário consiste no desenvolvimento e após a aplicação do mesmo a um público-alvo. Para Hill e Hill (1998), um bom questionário é fundamental para especificar os objetivos principais da pesquisa, os secundários, as hipóteses, as escalas de resposta e os métodos para coleta e a análise dos dados.

O roteiro para a criação do questionário segue de acordo com uma sequência de passos:

- Descrever os objetivos;
- Selecionar o público-alvo;
- Construir o questionário;
- Fazer uma aplicação pré-teste do questionário;
- Revisar o questionário;
- Aplicar o questionário;
- Codificar as respostas;

- Analisar e interpretar os dados;
- Preparar um relatório final.

O objetivo do questionário é realizar um levantamento referente à preocupação e aos cuidados que a empresa possui em relação à segurança da informação dentro da sua organização. Os objetivos secundários são analisar se ela tem conhecimento e entendimento das principais ameaças que sua organização possui hoje em dia e se ela já utiliza/conhece mecanismo para proteção de suas informações.

O público-alvo foi a empresa do estudo de caso e todas as pessoas que estão diretamente ligadas com as informações da mesma. O questionário é desenvolvido por perguntas fechadas e de múltipla escolha, isto é, apresenta várias alternativas ao respondente, restringindo as respostas, mas, ao mesmo tempo, facilitando a análise dos dados.

Após a elaboração do questionário, o mesmo será aplicado em uma versão preliminar com finalidade de identificar quaisquer adversidades que justifiquem modificações nas perguntas, alteração no formato do questionário ou até mesmo identificação de conteúdo a ser eliminado ou acrescentado na versão final do questionário.

Em seguida, foi realizada a revisão do questionário com o objetivo de ajustar os possíveis problemas identificados no pré-teste. Por fim, foi aplicado o questionário com validade para codificação, interpretação e compilação dos resultados. O esboço dos questionários que foram aplicados antes e depois do estudo de caso, consulte o apêndice B e apêndice C.

4.3 CONSIDERAÇÕES PARCIAIS

Este capítulo teve por objetivo detalhar a proposta de solução baseando-se nas pesquisas bibliográficas e levantamentos dos estudos descrito neste trabalho, bem como, exemplificar passo a passo da análise de riscos, mecanismos de

segurança e ferramentas que serão analisadas posteriormente na continuação deste trabalho.

5. ESTUDO DE CASO

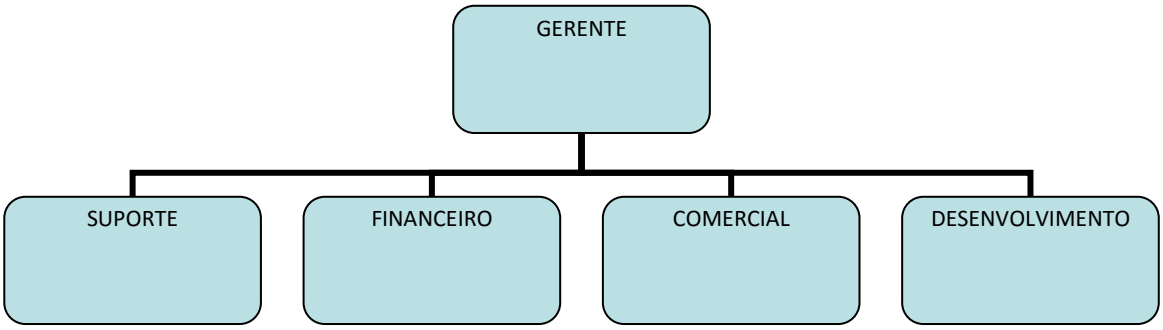
O estudo de caso, aqui apresentado, foi realizado numa empresa de pequeno porte e desenvolvedora de *softwares* a mais de 10 anos. Ela atua nos ramos de indústria, comércio e serviço.

5.1 CENÁRIO ATUAL

Para efeitos de segurança os dados da empresa, bem como toda a análise de riscos são preservados. Será divulgado apenas relações do levantamento. A empresa em questão será denominada neste estudo de XYZ.

A XYZ atua na região serrana e conta com mais de 140 clientes em sua carteira. A empresa por ser de pequeno porte, conta com o gestor e mais quatro colaboradores. O organograma da empresa é mostrado na Figura 5.

Figura 5 – Organograma da Empresa



Fonte: Próprio Autor

O gerente da empresa hoje participa em todas as funções da organização com foco na parte de desenvolvimento, customizações, melhorias e também nas atividades financeiras da empresa. Em paralelo ao gestor, a organização consta com duas pessoas na parte do suporte, o qual denomina-se nível 1 e nível 2. Nas funções comerciais, a organização conta com um colaborador, o qual está iniciando este ano com os trabalhos de venda dos produtos da empresa.

Além de suas funções, o próprio gestor também é responsável pela segurança das informações. Neste contexto, analisando brevemente os conhecimentos técnicos do gerente quanto a importância da segurança da informação, foram identificadas algumas características relevantes:

- Um *software* de antivírus, gratuito, que faz varreduras na rede em busca de vírus e *malwares*.
- A empresa possui 6 microcomputadores em plataformas Windows.
- O servidor da empresa possui plataforma Windows server 2008 R2.
- Licenças de *softwares*.

Em paralelo, alguns itens que facilitam ou tornam a organização vulnerável a ameaças foram detectados. Alguns aspectos negativos identificados no cenário atual são:

- O servidor encontra-se na mesma sala que os colaboradores, tornando-o assim vulnerável, pois o acesso não é restrito.
- Todos os computadores não têm bloqueio de mídias removíveis e possuem mídia CD/DVD.
- Todos os microcomputadores possuem acesso à internet sem nenhum bloqueio.
- A empresa não possui uma pessoa especializada na segurança da informação, comprometendo assim, o controle e monitoramento efetivo.
- A empresa não possui *firewall*, deixando vulnerável o controle de acessos e comunicação com internet.

Uma vez feito o levantamento autoral dos aspectos positivos e negativos da organização, fez-se necessário entender a percepção sobre segurança de todos os colaboradores da empresa. Para isso, um breve questionário foi elaborado (Apêndice B) e aplicado a todos os funcionários e ao gestor da empresa com intuito de auxiliar no levantamento.

Como primeiro resultado detectou-se que as informações são gerenciadas e reconhecidas como um recurso estratégico de grande importância para a empresa e seus clientes. Mesmo com planejamento de forma integrada quanto a gestão de suas informações, a empresa atualmente prioriza outros critérios ante a segurança da informação.

Em relação ao apoio gerencial da empresa, hoje ela não tem os processos documentados e também as informações não estão centralizadas. Ao mesmo tempo que possuem banco de dados, também existem outros controles paralelos realizados através de papéis, documentos eletrônicos não documentados e outras mídias removíveis.

A empresa possui processos pequenos e não utiliza normas nem políticas para controlar suas informações, porém dispõe de termos ativos de confidencialidade a todos seus colaboradores, garantindo o comprometimento com o sigilo das informações.

Uma dificuldade levantada no questionário foi, que a empresa não tem uma visão clara dos riscos e ameaças que ela está vulnerável diariamente. Diante disso, ela admite que já sofreu problemas com falhas de segurança ocasionando roubo da informação e quebra de confidencialidade.

Considerando os problemas já ocorridos pela empresa, os que tiveram maior impacto pela empresa foram processamento ilegal dos dados, defeito de *software* e uso não autorizado de equipamentos. Para tanto, foi questionado se a empresa utiliza algumas ferramentas disponíveis no mercado que auxiliam na prevenção destes e outros incidentes. A empresa somente utiliza mecanismos de cópias de segurança, certificado digital e antivírus (gratuito).

De forma comparativa, os aspectos positivos e negativos levantados anteriormente se equiparam com as conclusões do questionário. Neste sentido, é visível que a empresa tem conhecimento e preocupação em relação as suas informações, porém utiliza poucas ferramentas e mecanismos na proteção delas.

5.2 ANÁLISE DE RISCO

A análise de risco é o ponto inicial na gestão da segurança da informação. Esta análise é realizada para identificar quais ameaças são relevantes nos processos da organização e quais os riscos associados. Na análise deste estudo de caso, foi utilizada a metodologia qualitativa da norma ABNT NBR ISO/IEC 27005:2011.

De acordo com a norma é necessário realizar o levantamento dos ativos e identificar as vulnerabilidades e ameaças, a fim de equilibrar o custo de um incidente e o custo das medidas de segurança.

Devido ao porte da empresa XYZ e baixa complexidade dos processos, a análise da gestão de riscos foi aplicado em todos os processos da empresa. Sendo alguns deles compras, vendas, análise, desenvolvimento, suporte e atendimento ao cliente.

Esta análise é indispensável para identificar as necessidades da empresa em relação às condições de segurança da informação e para criar um sistema de gestão de segurança da informação eficiente. A análise de risco foi dividida nas seguintes etapas:

- Definição do contexto.
- Identificação dos ativos.
- Identificação das ameaças.
- Identificação dos controles existentes.
- Identificação das vulnerabilidades.
- Identificação das consequências.
- Estimativa dos riscos.

Em uma primeira etapa desta análise, avaliou-se os processos principais da empresa onde foram identificados quatorze ativos. Após este levantamento inicial,

todos os ativos foram classificados em grupos, sendo eles: *software*, *hardware*, humanos e instalações prediais. Foi dividido em grupos para uma análise mais simples e para melhor entendimento dos ativos selecionados da empresa.

Após a classificação dos ativos, foi realizada a análise das ameaças encontradas em cada ativo. Neste ponto do diagnóstico, encontrou-se um total de setenta e duas ameaças diretamente ligadas aos ativos da empresa. Todas estas ameaças também foram classificadas de acordo com sua origem (interna/externa) e o tipo desta ameaça (acidental / intencional / desastre natural).

Nota-se que dentre todas as ameaças encontradas, a maioria ficou concentrada no grupo dos ativos classificados como *software*, com um total de trinta e seis ameaças, sendo que destas, vinte e cinco são do tipo internas/externas. O Quadro 11 apresenta um resumo desta análise, quantificando as ameaças encontradas pelo tipo de ativo e a origem de sua ameaça.

Quadro 11 – Relação de ameaças por grupo de ativos

Tipo Ameaça/Ativo	*Software*	*Hardware*	Instalações prediais	Humanos
Interna/Externa	25	14	6	1
Interna	3	1	-	11
Externa	8	3	-	-
Total	**36**	**18**	**6**	**12**

Fonte: Elaborada pela autora

O Quadro 12 quantifica o número de ameaças pelo tipo de ativo e pela origem da ameaça. Os maiores números de ameaças foram acidentais ou intencionais, totalizando vinte e duas ocorrências. Apenas doze foram encontradas no grupo humanos e seis em instalações prediais.

Quadro 12 – Origem das ameaças por grupo de ativos.

Origem da ameaça/Ativo	*Software*	*Hardware*	Instalações prediais	Humanos
Acidental/Intencional	12	5	1	4
Intencional	10	4	-	2
Acidental/Natural	3	2	-	1
Natural	5	1	-	3
Acidental/Natural/Intencional	1	4	3	1
Natural/Intencional	3	2	2	1
Natural/acidental	2	-	-	-
Total	**36**	**18**	**6**	**12**

Fonte: Elaborada pela autora

Após a etapa de levantamento das ameaças, o próximo passo é a análise dos controles existentes. Foram analisados e mensurados todos os controles existentes atualmente na organização, classificando-os em planejado/existente. Além desta classificação, a situação da implementação dos controles também foi considerada: adequada e necessita revisão.

No final da análise, foram encontrados doze controles existentes nos processos atuais da empresa. Destes controles, todos são existentes, nenhum planejado. Entre os doze controles implementados, sete deles necessitam de revisão. Os dados coletados podem ser consultados no Quadro 13.

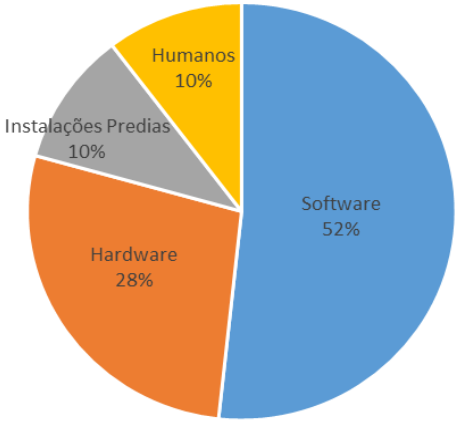
Quadro 13 – Relação de controles por grupos de ativos

Ativos/Controles	Existentes	Planejados	Necessita Revisão
Software	6	-	3
Hardware	4	-	3
Instalações Prediais	1	-	-
Humanos	1	-	1
Total	12	-	7

Fonte: Elaborado pela autora.

De acordo com os dados analisados, os dois grupos que possuem maior quantidade de controles implementados (*software* e *hardware*) concentram mais de 80% das vulnerabilidades. Na Figura 6 resumem-se as vulnerabilidades de cada grupo:

Figura 6 – Relação das Vulnerabilidades



Fonte: Próprio Autor

A empresa não possui muitos controles internos devido ao seu porte. Nenhum desses controles possui documentação ou especificação técnica de sua implementação.

A próxima etapa da análise de riscos foi a identificação das consequências, isto é, avaliar os impactos/consequências nos negócios da organização decorrentes da violação da segurança. Foi criada uma lista com os possíveis cenários de incidentes, para cada ativo da empresa e identificadas as consequências. Foram encontrados treze incidentes e vinte e seis consequências. A maior parte desses incidentes está diretamente relacionado aos ativos de *hardware* e *software*.

Após o levantamento das consequências, foi realizada a análise das probabilidades e consequências (impactos). A norma ABNT ISO/IEC 27005:20011 não estabelece um método específico para avaliar as probabilidades. Neste estudo, utilizou-se a orientação da metodologia NIST SP 800-30 (2012), que sugerem que as probabilidades qualitativas sejam classificadas como:

- Alto: É quando a ameaça é altamente motivada, podendo de fato explorar a vulnerabilidade e cujos controles não forem eficazes.
- Médio: É quando a ameaça é motivada o suficiente para explorar uma vulnerabilidade, mas os controles podem prevenir que a mesma seja explorada.
- Baixo: É quando a ameaça não é motivada ou não é capaz de explorar uma vulnerabilidade, ou ainda há controles que podem prevenir ou impedir que a mesma seja explorada.

A metodologia NIST SP 800-30 (2012) também sugere que os impactos sejam classificados como de acordo com o Quadro 14:

Quadro 14 – Relação Riscos x Impactos

(continua)

Probabilidade	Impacto
1. Perda de recursos ou ativos	A. Gera um custo bastante elevado.
	B. Gera um custo elevado.
	C. Gera um custo razoável.

(conclusão)

2. Missão da instituição	A. Prejudica ou impede a missão da instituição de forma significativa.
	B. Prejudica ou impede a missão da instituição.
	C. Afeta a missão da instituição
3. Danos físicos	A. Causa lesões graves em pessoas ou morte.
	B. Causa lesões graves em pessoas.

Fonte: Elaborada pela autora.

- Alto: Se for enquadrado em pelo menos um dos itens da tabela: 1 – A, 2 – A ou 3 – A.
- Médio: Se não pertencer a classificação alta e for enquadrado em pelo menos um dos itens 1 – B, 2 – B ou 3 – B.
- Baixo: Se for enquadrado nos itens 1 – C e/ou 2 – C.

Para explicar melhor, o nível de risco da empresa XYZ, foi utilizada a estimativa qualitativa para demonstrar a expectativa de ocorrência de riscos. A matriz do Quadro 15 mostra os resultados obtidos após a avaliação da relação entre a probabilidade em um cenário de incidente e o impacto estimado, do ponto de vista do negócio. O nível do risco foi calculado considerando o nível do impacto em relação ao nível da probabilidade. Por exemplo, para cada vulnerabilidade, quando o risco foi baixo, este foi classificado com valores entre 0 – 2. As vulnerabilidades com risco médio, receberam valores entre 3 – 5, e os riscos classificados como alto, receberam valores entre 6 – 8.

Quadro 15 – Matriz de Riscos com valores pré-definidos

Probabilidade	**Impacto**	**A-Alta**	**B-Médio**	**C-Médio**
	Baixo	-	1	1
	Médio	7	10	1
	Alta	2	6	3

Fonte: Elaborada pela autora

Para cada grupo de ativo analisado foi encontrada uma média de quatro vulnerabilidades, o maior número novamente está concentrado nos ativos humanos da empresa.

Todas as vulnerabilidades levantadas ficaram com média similar nos níveis de riscos quando analisados os valores de maior e menor risco. Nota-se que os limites para a maioria dos ativos não atingem o seu nível máximo de risco e tão pouco o mínimo, haja vista os níveis 6 e 7 para valores máximos e 4 para valores mínimos, com exceção uma vulnerabilidade relacionada a humanos que foi considerado de nível alto, com nível de risco 8. O resumo dos dados levantados na análise de riscos é apresentado no quadro 16.

Quadro 16 – Análise de riscos da empresa XYZ

Ativo	Nº de Ativos analisados	Nº de Vulnerabilidades	Nível de Risco	
			Maior	Menor
Software	6	6	7	4
Hardware	3	4	6	4
Instalações Prediais	3	4	6	4
Humanos	2	2	8	4

Fonte: Elaborada pela autora

Todos os dados apresentados nesta seção foram extraídos da análise de riscos realizada na empresa XYZ, onde fica claro que, mesmos em processos simples e empresa de pequeno porte, com ativos diversos, existem várias ameaças e vulnerabilidades que passam despercebidas no dia a dia.

A análise também deixa claro que entre todos os ativos verificados as ameaças estão concentradas no grupo de ativos *software* e *hardware*, com grande percentual proveniente internamente e externamente, ocorrendo de forma acidental ou intencional. Origem de causas naturais representa um baixo percentual comparando com as demais origens.

O grupo humanos representa 16% das ameaças encontradas, em contrapartida, o baixo percentual contradiz com o maior nível de impacto perante a empresa. Isto significa que o grupo possui um número inferior de ameaças em relação aos demais grupos, porém, o risco que ele representa para a organização tem um impacto de grande significância, caso a vulnerabilidade venha ocorrer.

Com base nos dados coletados, conclui-se que, a organização está vulnerável tanto internamente quanto externamente. Por este motivo, é necessário implementar algumas ferramentas e mecanismos de segurança internos e externos, a fim de

regrar e proteger seus ativos relacionados as suas informações. Os resultados obtidos na análise de riscos foram satisfatórios, haja vista a possibilidade de cumprimento da proposta de minimização dos riscos os quais a empresa está vulnerável.

5.3 LEVANTAMENTO DOS MECANISMOS E FERRAMENTAS DE SEGURANÇA

Perante os dados levantados e analisados, a organização atualmente já utiliza alguns mecanismos de segurança e ferramentas já atuantes, porém é necessário implementar alguns processos e ferramentas para garantir ainda mais a confidencialidade e segurança das informações que são gerenciadas diariamente.

Para ajudar na proteção e prevenção contra *softwares* maliciosos como vírus e *worms* foi necessário revisar as configurações do antivírus atual, identificando que o mesmo estava defasado, desatualizado e não possibilitava criar políticas de segurança para cada usuário. Um novo antivírus foi adquirido, com licença comercial, *Kaspersky* Total *Security* 2018 multidispositivos, com valor de investimento inicial de R$160,93 por ano para 5 computadores. Dentre todos os *softwares* disponíveis no mercado, este *software* teve maiores pontuações em sítios de qualificações, direcionados a empresas de pequeno e médio porte. Ele oferece maior segurança nas transações bancárias, atividade a qual a empresa realiza diariamente. Outro ponto positivo que pesou na escolha foi a possibilidade de monitorar as atividades de cada colaborador permitindo, por exemplo, o bloqueio de qualquer site, caso a utilização for considerado inapropriada, sendo bem funcional à qualquer usuário leigo.

Foi adquirido 5 licenças do *software* e configurado em todas as estações da empresa. Após instalação, foi revisado as permissões de acesso de cada usuário e ajustado para cada conta.

Outra ferramenta foi um mecanismo de segurança responsável pelo controle de tráfego de rede. A ferramenta definida para realizar este controle é o *Wireshark*, permitindo o controle de tráfego de toda a rede em tempo real, com fácil manuseio e

sem nenhum custo de implementação. Como as atividades que necessitam utilizar a internet são crescentes, é necessário realizar monitoramentos constantes. Além do fator produtividade, o tráfego da rede precisa ser balanceado para que os sistemas que executam não fiquem lentos para quem está utilizando. A instalação e configuração deste mecanismo foi simples. Agora o gestor da empresa consegue acompanhar em tempo real todo o tráfego de rede, emitir relatórios gerenciais por usuário e melhorar os controles de acessos de cada usuário.

No levantamento de riscos também foi identificado deficiência do atual *software* de cópias de segurança, onde foi definido a necessidade de implantação de um novo *software* mais robusto. Por se tratar de um *software* com custo anual, optou-se na aquisição de apenas uma licença, com valor de US$469,00/ano para o servidor da empresa. Apesar de conter um valor inicial um pouco elevado ele conta com várias vantagens até então inexistentes no antigo *software* de *backup.*

O ***software*** de backup selecionado foi o *Acronis True Image*. A aquisição e instalação deste *software* foi simples e intuitiva, sem nenhuma complicação ou necessidade de conhecimento técnico por parte do usuário. Algumas vantagens pelas quais optou-se por este *software* foi a possibilidade de realizar *backups* diferenciais e incrementais, isto é, o *software* identifica apenas as mudanças feitas no último *backup*, reduzindo significativamente o tempo de backup e o uso da rede. Com isso, ele permite recuperar parte de arquivos/pastas sem a necessidade da recuperação do *backup* inteiro.

Para as demais estações clientes foi padronizado o *software* gratuito já utilizado pela empresa, tendo em vista que os colaboradores já estavam familiarizados (*Iperius Backup*). Ficou definido um processo de verificação de backup semanal a fim de verificar se o procedimento de cópia de segurança está sendo realizado corretamente.

Outro ponto identificado foi a precariedade nas senhas dos produtos, contas e sistemas que os colaboradores utilizam diariamente. Com o intuito de aumentar a segurança da informação de seus dados, definiu-se a elaboração e recadastramento de novas senhas com alguns padrões pré-determinados internamente para ampliar a proteção. Com isso, estabeleceu-se que todas as senhas de e-mails, *Skype*, usuários dos sistemas e acessos internos devem conter no mínimo de oito

caracteres, dentre eles letras maiúsculas, minúsculas e obrigatoriamente um caractere especial.

No início notou-se certa resistência pela parte dos colaboradores devido ao grande trabalho que teriam pela frente, complexidade e obrigatoriedade da mudança. O tempo para criar as novas senhas foi um pouco elevado devido a desconfiança dos colaboradores. Após o procedimento ter finalizado, os colaboradores notaram que realmente existiam falhas nas suas próprias senhas, percebendo assim, a necessidade da troca.

A empresa já possui um mecanismo fundamental para um bom andamento de seu negócio, o termo de responsabilidade e confidencialidade das informações geridas. Entretanto foi identificado algumas lacunas as quais poderiam ser aprimoradas. Após análise do termo atual da empresa, junto com o gestor da empresa, foi elaborado melhorias nas cláusulas deste documento a fim de minimizar os incidentes sobre a quebra de sigilo. Com isso, foi possível atualizar os funcionários sobre seu comprometimento perante a empresa, seu compromisso de manter a confidencialidade e sigilo sobre todas as informações jurídicas e técnicas relacionadas ao seu cargo, função ou atividade.

Outro mecanismo que foi analisado e implementado na empresa foi a habilitação do filtro de spam de e-mails. A empresa não tinha conhecimento desta possibilidade de configuração do filtro de spam em seus e-mails gratuitamente. Com isso, foi habilitado este filtro que é composto por um conjunto de regras, fatores e algoritmos que classificam a mensagem entrante como legítima ou não.

O *software* de criptografia *AxCrypt* também foi implementada na organização com intuito de criptografar os principais arquivos da empresa. A empresa realizou o levantamento de quais arquivos necessitariam de criptografia e após foi selecionada a ferramenta para realizar este serviço. Um dos pontos positivos para a escolha desta ferramenta foi por se tratar de um *software opensource* e de fácil utilização.

5.4 AVALIAÇÃO DAS FERRAMENTAS IMPLANTADAS

O novo antivírus, além de novas funcionalidades, trouxe maior proteção à empresa. Diariamente ele “escaneia” as máquinas, alerta para possíveis ameaças, direcionando os arquivos infectados para quarentena.

Através da criação das regras de acessos da internet, foi possível perceber certa resistência pela parte dos colaboradores, pois antes todas as páginas estavam liberadas, e agora algumas delas foram bloqueadas. A gerência tomou essa decisão pois, diariamente, *softwares* indesejados estavam sendo instalados automaticamente nos dispositivos, *softwares* que não eram necessários para desenvolver as atividades da empresa.

O *software* de controle de tráfego de rede tem uma interface que apesar de, ser em inglês, é intuitiva e com uma estrutura bastante prática. O programa é dinâmico permitindo a instalação de alguns componentes, *plugins* e bibliotecas. Todo o tráfego de entrada e saída é analisado e mostrado em uma lista com diversos recursos de navegação. Com alguns relatórios e pouco conhecimento em redes, o gestor conseguiu monitorar sua rede de dados e entender melhor tudo o que passava por ela diariamente.

A maneira de gerenciar e monitorar as cópias de backup não teve grande mudança, apenas sofreu mudança de sistema e algumas funcionalidades imperceptíveis ao usuário. O backup foi configurado para executar duas tarefas diariamente e ficou definido que cada mês uma pessoa diferente é responsável em verificar semanalmente se o backup foi executado sem nenhum erro. Nenhuma grande dificuldade foi encontrada nesta ferramenta, todos os colaboradores e o gestor da empresa tem conhecimento básico para gerenciar este *software*, que também é bem intuitivo.

As senhas estavam defasadas e não seguiam nenhum padrão. A reformulação da política de senhas buscou maior segurança nos principais acessos da empresa.

O termo de responsabilidade e confidencialidade foi reformulado com intuito de atualizar as políticas da empresa e conscientizar os colaboradores sobre as novas regras. O novo termo estabelece os objetivos da empresa, as

responsabilidades que os colaboradores possuem com as informações da empresa e do cliente.

O filtro spam foi um mecanismo básico e fácil de implementar, até então desconhecido pela empresa, e teve resultados percebíveis para seus usuários devido a sua funcionalidade de filtragem. Foi notável a filtragem de conteúdo na entrada de e-mails, avaliando a probabilidade de que as mensagens são legítimas ou spam. Isto auxiliou na separação de e-mail legítimos (com importância) contra os diversos e-mails de spam que cada usuário recebia diariamente.

Na criptografia dos arquivos individuais, optou-se por criptografar alguns dados mais relevantes ao negócio da empresa. A ferramenta escolhida tem integração avançada com o sistema operacional (*Windows*), onde é necessário apenas clicar sobre um arquivo para criptografá-lo. A ferramenta ainda conta com funções como apagar o arquivo completamente do disco, sendo impossível recuperá-lo, e bloqueio com senha, um arquivo-chave ou ambos. Ela também é compatível com serviços de sincronização na nuvem, como o *Dropbox*, Google Drive e *SkyDrive*. O *AxCrypt* ainda permite um armazenamento e compartilhamento de fácil manuseio dos arquivos criptografados.

5.5 APLICAÇÃO FINAL DO QUESTIONÁRIO

Nesta fase final do estudo de caso foi aplicado um questionário com o intuito de compreender como foi a aplicação das ferramentas pela visão da empresa, quais foram as maiores dificuldades e como foi a aceitação do desafio por toda a equipe. Como resultados, o questionário demonstrou que as ferramentas propostas tiveram grande aceitação por todos os profissionais da empresa encontrando apenas algumas dificuldades. Algumas resistências foram encontradas durante o percurso, porém nada que pudesse impedir a continuidade do trabalho.

Na análise, também ficou visível que alguns colaboradores desconheciam algumas ferramentas que foram apresentadas e implantadas dentro da organização, porém, dia a dia, eles buscaram entender as funcionalidades das mesmas para que elas pudessem auxiliá-los no gerenciamento.

Por fim, a empresa sugeriu algumas melhorias que possam aperfeiçoar ainda mais as brechas na segurança das informações dentro da organização, bem como, os profissionais se propuseram a buscar ferramentas constantes.

5.6 CONSIDERAÇÕES FINAIS

Os resultados finais da análise de riscos levantados na empresa XYZ demonstraram que existem riscos dentro da organização, independentemente do seu porte, ignorá-los não os farão desaparecer. Todos os grupos analisados possuem ameaças diretamente ligadas a seus ativos. Os maiores riscos identificados estão diretamente vinculados aos grupos de *software* e *hardware*, tornando possível implementar mecanismos de segurança para minimizar os incidentes. Também foi necessário aplicar algumas mudanças relacionadas aos grupos humanos, pois são eles que estão em contato com todas as informações da empresa diariamente, orientando e disciplinando os usuários. Além da empresa já possuir alguns controles, nenhum deles possui documentação.

A implementação das ferramentas e mecanismos de segurança além de documentar e padronizar os controles já existentes na organização, visam proteger contra as ameaças e vulnerabilidades que os ativos possuem. Desta forma, foi implementado todas as ferramentas e mecanismos citados neste capítulo.

Após a aplicação e avaliação dos mecanismos e ferramentas aplicadas foi possível verificar aspectos e pontos de vistas diferentes. Todos os colaboradores e o gestor participaram das definições e transformações da empresa e conseguiram identificar a importância da segurança da informação no âmbito corporativo, apesar de possuir certa resistência na aplicação de alguns mecanismos. O retorno da direção foi bem positivo sendo que, além das ferramentas sugeridas e implementadas, foi sugerido algumas melhorias e adequações para as ferramentas. Este trabalho não pretende encerrar a implementação das ferramentas na empresa, uma vez que, as ferramentas estão em constantes atualizações e novas tecnologias surgem diariamente. Além disso, é necessário também realizar um trabalho constante de conscientização de todos os colaboradores, parceiros de negócios e outros que se relacionem diretamente com os ativos de informação da organização.

6. CONCLUSÕES

A informação tornou-se imprescindível dentro das organizações. Os controles que antes eram realizados manualmente, foram automatizados e sistematizados. Com essa evolução tecnológica as empresas ficaram dependentes da tecnologia, necessitam proteger suas informações pois elas se tornaram principal ativo dentro das organizações.

O presente trabalho teve por objetivo analisar os principais tipos de ataques, ameaças, mecanismos de segurança e ferramentas relacionadas com a quebra de confidencialidade. Primeiro foi necessário realizar um estudo sobre conceitos de segurança de informação, ciclo de vida, ameaças, mecanismos e ferramentas de segurança da informação encontradas na literatura.

No decorrer do estudo foi necessário aplicar um questionário aos envolvidos da empresa para entender a percepção sobre segurança da informação. Neste levantamento ficou visível que a empresa tem conhecimento e preocupação em relação as informações geridas diariamente, porém utiliza poucas ferramentas e mecanismos na proteção. Após, uma análise de risco foi realizada, onde verificou-se que 16% das ameaças estudadas estavam diretamente ligadas aos ativos humanos. Dentre as origens avaliadas, 22% delas foi constatado que acontece de forma intencional. Conclui-se que a organização possui vulnerabilidades e que necessitava de algumas ferramentas e mecanismos para auxiliá-la na proteção de suas informações. Ainda não foi possível medir os resultados das ferramentas implantadas, pois nesse período ainda não ocorreram problemas de segurança. O único resultado concreto foi a maior conscientização dos colaboradores da empresa em relação a segurança e a importância de ser um profissional ético.

Diante deste estudo, é valido pré-julgar que os problemas enfrentados pela empresa XYZ retratam uma realidade muito presente em todas as pequenas, médias e até grandes empresas que, na falta de um departamento que gerencie a segurança da informação, deixe seus ativos a mercê de ataques cada vez mais frequentes. Estendendo esta realidade, pode-se afirmar que a segurança da informação atualmente é pouco explorada pelas empresas de pequeno porte, sendo que, a implementação é vista como um gasto e dor de cabeça. Além disso, também

ficou nítido perceber a evolução do pensamento e conhecimento de todos os colaboradores da empresa referente a importância da segurança da informação no âmbito corporativo, conscientizando-se do bem precioso o qual eles trabalham diariamente.

Em linhas gerais, no estudo de caso foi desenvolvida uma solução de acordo com a análise de risco e com as ameaças encontradas na literatura. Em resumo, as maiores incidências de ameaças encontradas dentro da empresa XYZ foram: acesso não autorizado das informações, processamento ilegal dos dados, defeito de hardware e software, cópia não autorizada das informações, dano físico à mídia, espionagem interna e externa e ataque à rede.

Este trabalho mostra que, na verdade, não é preciso grandes investimentos para que a informação esteja mais segura. A empresa precisa querer proteger seus dados, efetuar os investimentos de acordo com sua cultura, necessidade e estrutura. Por fim, conclui-se que as ferramentas certas implementadas com eficiência minimizam as chances de quebra de confidencialidade dentro das organizações.

6.1 RECOMENDAÇÕES

Buscando aplicar este trabalho, uma das sugestões de continuação é realizar uma nova avaliação dos riscos e separando-os pelos principais processos da organização. Outro ponto que pode ser importante realizar é a aplicação do estudo de caso em empresas de micro e/ou pequeno porte que atuem em outras áreas, validando assim, outros ambientes corporativos. Testar as ferramentas e mecanismos em outros ambientes organizacionais para poder efetuar algumas comparações de cada gestão adotada das empresas.

REFERÊNCIAS BILIOGRÁFICAS

ABNT **NBR ISO/IEC 27002: Tecnologia de informação:** Técnicas de segurança - Código de prática para controles de segurança da informação. 2 ed. Rio de Janeiro: Abnt, 2013.

ABREU, Leandro Farias dos Santos. **A segurança da informação nas redes sociais,** 2011. Disponível em: < http://docplayer.com.br/104810-Faculdade-de-tecnologia-de-sao-paulo.html>. Acesso em: 09 de Abril de 2017.

ALBURQUERQUE, Ricardo; RIBEIRO, Bruno. **Segurança no desenvolvimento de Software**. Rio de Janeiro: Editora Campus Ltda, 2002.

AUDY, Jorge Luis Nicolas; ANDRADE, Gilberto Keller de; CIDRAL, Alexandre. **Fundamentos de Sistemas de Informação.** São Paulo: Artmed Editora S.A., 2005.

COMPUTEREORLD. **Yahoo revela novo vazamento de dados que afetou 1 bilhão de usuários.** Dez. 2016. Disponível em: <http://computerworld.com.br/yahoo-revela-novo-vazamento-de-dados-que-afetou-1-bilhao-de-usuarios>. Acesso em: 28 de fevereiro de 2017.

COMPUTEREORLD. **Vazamento na Experian expõe dados de 15 milhões de consumidores nos EUA.** Out. 2015. Disponível em: <http://computerworld.com.br/vazamento-na-experian-expoe-dados-de-15-milhoes-de-consumidores-nos-eua>. Acesso em: 27 de fevereiro de 2017.

COMPUTERWORLD. **Proteção de e-mails corporativos será tendência em 2017**. Dez. 2016. Disponível em: <http://computerworld.com.br/protecao-de-e-mails-corporativos-sera-tendencia-em-2017>. Acesso em: 08 de março de 2017.

COMPUTERWORLD. **Perdas de empresas brasileiras com incidentes de segurança chega a US$ 1 mil.** Janeiro de 2017. Disponível em: <http://computerworld.com.br/perdas-de-empresas-brasileiras-com-incidentes-de-seguranca-chegam-us-1-mi>. Acesso em: 10 de março de 2017.

COSTA, Clovis Corrêa da. **Estratégia de negócios.** São Paulo: Saraiva, 2009.

DRESCH, Aline; LACERDA, Daniel Pacheco; JÚNIOR, José Antonio Valle Antunes. **Design Science Research**: métodos de pesquisa para avanço da ciência e tecnologia. Porto Alegre: Bookman, 2015.

FLOWERDAY, Stephen V.; TUYIKEZE, Tite. **Information security policy development and implementation: The what, how and who.** South Africa: Elsevier, 2016.

FONTES, Edison. **Segurança da Informação: O Usuário faz a diferença.** São Paulo: Saraiva, 2006.

GALLAGHER, Patrick D.. **NIST National Institute of Standards and Technology.** United States Of America, 2012.

GALVÃO, Michele da Costa. **Fundamentos em Segurança da Informação**. São Paulo: Person Education do Brasil, 2015.

HILL, Manuela Magalhães; HILL, Andrew. **A construção de um questionário**. Disponível em: <http://dinamiacet.iscte-iul.pt/wp-content/uploads/2012/01/DINAMIA_WP_1998-11.pdf> Acesso em: 10 de junho de 2017

INTECO, National Institute for Communications Technologies. **Taxonomy information security taxonomy handbook.** León, Espanha: Gráfica Alse. Fevereiro de 2010.

LANDIM, Wikerson. **Snapchat é hackeado e dados de 4,6 milhões de usuários são expostos.** Janeiro de 2014. Disponível em: <https://www.tecmundo.com.br/ataque-hacker/48625-snapchat-e-hackeado-e-dados-de-4-6-milhoes-de-usuarios-sao-expostos.htm>. Acesso em: 08 de março de 2017.

LAUREANO, Marcos Aurelio Pchek.**Gestão de Segurança da Informação**, 2005. Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em: 19 de março de 2017.

MACÊDO, Diego. **Modelos e mecanismos de segurança da informação**, 2014. Disponível em: <http://www.diegomacedo.com.br/modelos-e-mecanismos-de-seguranca-da-informacao/>. Acesso em: 15 de Abril de 2017.

MALIN, Ana Maria Barcellos. **Gestão da Informação Governamental: em direção a uma metodologia de avaliação.** Datagamazero - Revista de Ciência da Informação, 2006.

OLIVEIRA, Wilson José de. **Segurança da Informação**: Técnicas e Soluções. Florianópolis: Visual Books Ltda, 2001.

Os critérios da informação pela perspectiva da segurança. Dezembro de 2016. Disponível em: < https://www.portalgsti.com.br/2016/11/cid-confidencialidade-integridade-e-disponibilidade.html> Acesso em: 19 de março de 2017.

SANTANA, Raimundo Alexandrino de. **Os Firewalls e a segurança na internet**, 2013. Disponível em: <https://pt.slideshare.net/alexandrino1/tcc-firewalls-e-a-segurana-na-internet>. Acesso em: 27 de março de 2017.

SÊMOLA, Marcos. **Gestão da Segurança da Informação,** uma visão Executiva. Rio de Janeiro: Elsevier, 2003.

SHIREY, R. RFC 2828 – **Internet Security Glossary. The Internet Society**, 2000. Disponível em: <http://www.ietf.org/rfc/rfc2828.txt?number=2828>. Acesso em: 19 de março de 2017.

STALLINGS, William. **Criptografia e segurança de redes.** São Paulo: Pearson Prentice Hall, 2008.

STALLINGS, William. **Network Security Essentials: Applications and Standards.** New Jersey: Pearson Education, 2003, 2ª Edição.

TADEU, Erivelto. **Empresas brasileiras perdem média de US$1 milhão com incidentes de segurança.** Disponível em:<http://idgnow.com.br/ti-corporativa/2017/01/23/empresas-brasileiras-perdem-media-de-us-1-milhao-com-incidentes-de-seguranca/>. Acesso em: 15 de março de 2017.

TRIBUNAL DE CONTAS DA UNIÃO. **Boas práticas em segurança da informação** /– 2. ed. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2007. Disponível em: <http://portal3.tcu.gov.br/portal/page/portal/TCU/comunidades/biblioteca_tcu/biblioteca_digital/BOAS_PRATICAS_EM_SEGURANCA_DA_INFORMACAO_0.pdf>. Acesso em: 03 de março de 2017.

XIMENES, Sérgio**. Minidicionário Ediouro da língua portuguesa**. 2. ed. reform. São Paulo: Ediouro, 2000.

APÊNDICE A - FERRAMENTAS DE SEGURANÇA DA INFORMAÇÃO

Atualmente podemos encontrar diversas ferramentas no mercado, algumas gratuitas, outras pagas e também *OpenSource* (código aberto) que auxiliam a proteger tais ameaças.

Abaixo pode-se analisar tais mecanismos de segurança relacionadas com suas ferramentas. Este levantamento tem por base a pesquisa virtual em sites de classificação qualitativa de *softwares*.

Firewall: ele monitora o tráfego de entrada e saída, possui defesa de rede, defesa proativa, oferece dois modos (básico e avançado), permite quais programas podem acessar a internet e quais devem ser bloqueados e outros. Tem suporte para os principais sistemas operacionais (Windows, Linux e OS X).

Ferramentas	**SO**	**Tipo Distribuição**	**Sítio**
ZoneAlarm Firewall	Windows 10/8/7, Vista, XP e Linux	Pago / Gratuito	https://www.zonealarm.com/software/free-firewall/
Comodo Internet Security	Windows 10/8/7 e Linux	Pago / Gratuito	http://www.comodobr.com/firewall/comodo_firewall.php
Iptables	Linux	Gratuito	https://www.netfilter.org/downloads.html

Controle de tráfego de rede: permite aos usuários monitorar o tráfego de entrada e saída separadamente. Também extrai um gráfico para indicar o fluxo. Algumas ferramentas têm gerenciamento de patches: corrigem vulnerabilidades antes de um ataque. Avaliação de vulnerabilidades. Gerenciamento de toda a sua rede com análises e estatísticas.

Ferramentas	SO	Tipo Distribuição	Sítio
NLoad	Linux e Unix	Gratuito	https://www.linuxdescomplicado.com.br/2014/12/10-ferramentas-para-monitorar-largura.html
GFI LanGuard	Windows, MAC e Linux	Gratuito / Pago	https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard
Microsoft Network Monitor	Windows	Gratuito	https://www.microsoft.com/en-us/download/details.aspx?id=4865

Sistemas e ferramentas de Criptografia: protegem o disco rígido através de criptografia, restringindo o uso de arquivos apenas ao administrador. Usam algoritmos fortes para garantir sigilo no acesso e afastar usuários maliciosos. Conseguem proteger arquivos e pastas no disco local, em memórias USB, CDs, DVDs, HDs externos e também na nuvem (Dropbox, Google Drive e Microsoft OneDrive). Este cofre virtual utiliza algoritmo AES-XES de 384 bits para criptografar os arquivos, oferecendo a criptografia mais avançada desta lista.

Ferramentas	SO	Tipo Distribuição	Sítio
Comodo Disk Encryption	Windows	Gratuito	https://www.comodo.com/news/press_releases/10_03_09.html
Steganos Safe	Windows	Pago	https://www.steganos.com/de/
VeraCrypt	Windows / OS X/ Linux	OpenSource / Gratuito	https://veracrypt.codeplex.com/

Autenticação: possui diversos modos os quais certificam o mecanismo de segurança de autenticação, tal como Certificado digital, tokens e identificadores biométricos. Certificado digital trata-se de um documento eletrônico com assinatura digital que contém dados como nome do utilizador (que pode ser uma pessoa, uma empresa, uma instituição, etc.), entidade emissora, prazo de validade e chave pública. Com o certificado digital, a parte interessada obtém a certeza de estar se relacionando com a pessoa ou entidade esperada. Token é um dispositivo eletrônico gerador de senhas, geralmente sem conexão física com o computador, podendo também, em algumas versões, ser conectado a uma porta USB. Um sistema biométrico analisa uma amostra de corpo do usuário. No caso do olho, ele analisa

265 pontos diferentes para formar uma imagem que será usada para comparação toda vez que o usuário tentar se autenticar.

Ferramentas	SO	Tipo Distribuição	Sítio
Certificados Digitais – Caixa Econômica Federal	Windows 7 / 8 e 10	Pago	http://www.caixa.gov.br/empresa/identidade-digital/Paginas/default.aspx
Tokens	-	Pago / Gratuito	
Identificadores biométricos	-	Pago	

Cópias de segurança: são *softwares* de backups que permitem que o administrador do sistema possa configurar um único servidor de backup para fazer backup de outros hospedeiros na rede para unidades de fita ou disco – modelo cliente/servidor. Realiza backup completo, diferencial e incremental. Alguns *softwares* permitem recuperar exatamente o que você precisa, de forma rápida e sem esforço, a qualquer hora, em qualquer lugar. Você escolhe onde e como fazer backup: local ou on-line.

Ferramentas	SO	Tipo Distribuição	Sítio
Advanced Maryland Automatic Network Disk Archiver – AMANDA	Linux	Gratuito	http://www.amanda.org/
Acronis True Image	Windows	Pago	http://www.acronis.com/en-us/personal/computer-backup/?gclid=CO6pjZaHu9MCFQ0GkQodh-QPsA
NovaBackup	Windows e Linux	Gratuito e pago	http://www.novastor.com/

Anti-Malware: detecta e remove malware em tempo real com avançada tecnologia anti-malware, anti-spyware e anti-rootkit. Analisa automaticamente as ameaças mais recentes. Interrompe ransomware desconhecido e conhecido com tecnologia patenteada da próxima geração que funciona proativamente para proteger seus arquivos. Detecta e impede o contato com sites falsos e links maliciosos.

Ferramentas	SO	Tipo Distribuição	Sítio
Malwarebytes	Windows	Gratuito / Pago	https://br.malwarebytes.com/
IOBit Malware Fighter	Windows	Gratuito	http://www.iobit.com/en/malware-fighter.php
ClamAV para Linux	Linux	Gratuito / Open Source	https://www.clamav.net/

Esteganografia: é um programa que é capaz de esconder dados em vários tipos de arquivos de áudio e de imagem. As frequências de som e de cor, respectivamente, não são alteradas tornando o arquivo resistente contra testes estatísticos de primeira ordem.

Ferramentas	SO	Tipo Distribuição	Sítio
Image Steganography	Windows	Gratuito	https://imagesteganography.codeplex.com/
Steghide	Linux	Gratuito	https://www.vivaolinux.com.br/artigo/Esteganografia-utilizando-steghide

Antivírus: ele detecta, impede e atua na remoção de programas de *software* maliciosos, como vírus e *worms*. São programas usados para proteger e prevenir computadores e outros aparelhos de códigos ou vírus, a fim de dar mais segurança ao usuário.

Ferramentas	SO	Tipo Distribuição	Sítio
McAfee	Windows, MAC OS X	Pago / Gratuito	https://secure.mcafee.com/us/index.html
Norton	Windows, MAC OS X	Pago	https://br.norton.com/
Panda	Windows, MAC OS X	Pago	http://www.pandasecurity.com/brazil/?ref=menu

Virtual Private Network (VPN): Virtual Private Network – VPN, é uma forma de conectar dois computadores utilizando uma rede pública, como a Internet. É preciso criar alguns mecanismos de segurança para que as informações trocadas entre os

computadores de uma VPN não possam ser lidas por outras pessoas. A proteção mais utilizada é a criptografia, pois essa garante que os dados transmitidos por um dos computadores da rede sejam os mesmo que as demais máquinas irão receber.

Ferramentas	SO	Tipo Distribuição	Sítio
ExpressVPN	Windows, Mac e Linux	Pago	https://www.expressvpn.com/pt
NordVPN	Windows, Mac e Linux	Pago	https://nordvpn.com/pt/
PureVPN	Windows e Mac	Pago	https://www.purevpn.com/servers-review-special.php

Sistema de detecção de intrusão: realiza a análise de tráfego e captura de pacotes em tempo real em redes que utilizam o protocolo IP. Ele pode analisar protocolos, buscar por conteúdo específico e pode ainda ser utilizado para detectar uma variedade de ataques e sondas, tais como: buffer overflows, ataques de CGI, tentativas de identificação de sistema operacional, entre outros.

Ferramentas	SO	Tipo Distribuição	Sítio
SNORT	Windows / Linux / Open Source	Gratuito	https://www.snort.org/
OSSEC-HIDS	Linux / Windows	Gratuito	http://ossec.github.io/

Gestão de Identidade: gerenciamento de identidade oferece uma escalabilidade inovadora com soluções sendo que reduz os custos operacionais e protege aplicativos e dados sensíveis - independentemente de estarem hospedados em instalações ou na nuvem. Esta ferramenta auxilia os departamentos de TI a protegerem o acesso a aplicações e recursos no data center empresarial e na cloud, fornecendo níveis de validação adicionais como a autenticação multifator e políticas de acesso condicional. A monitorização de atividades suspeitas através de relatórios de segurança avançados, auditoria e alertas ajuda a mitigar problemas de segurança potenciais.

Ferramentas	SO	Tipo Distribuição	Sítio
Gerenciamento de identidade e acesso Oracle	-	Pago	https://www.oracle.com/middleware/identity-management/index.html
Gestão de identidades e acessos – Microsoft	Windows	Pago	https://www.microsoft.com/pt-pt/cloud-platform/azure-active-directory

Dispositivos de proteção física de equipamentos: pode-se citar os cabos de aço antifurto protegendo o equipamento.

APÊNDICE B - INSTRUMENTO DE COLETA DE DADOS INICIAL

Este questionário será aplicado no início do estudo de caso e tem por intuito analisar as preocupações da empresa e de seus colaboradores em relação às informações gerenciadas diariamente.

A avaliação poderá ser classificada em cinco níveis:

< 0 > - Não aderente, quando a empresa não realiza nenhuma ação em suas operações, não possui nenhuma preocupação.

< 1 > - Empresa desenvolveu alguma vez a ação e forma isolada e desestruturada, adesão da minoria.

< 2 > - A empresa vem desenvolvendo ações e é pouco estruturada, apenas parte da organização compreende e adota.

< 3 > - Empresa vem regularmente desenvolvendo ações, porém ainda falta articulação e integração no nível organizacional, maior parte da organização compreende e adota ainda que exista resistência.

< 4 > - A empresa vem desenvolvendo ações sistemáticas, estruturadas e integradas em toda empresa, está totalmente de acordo com a realidade da empresa.

As questões a seguir têm por objetivo analisar a cultura e práticas da organização referente ao gerenciamento e planejamento de suas informações.

1. Costumes informacional necessária para promover e sustentar o gerenciamento da informação.	0	1	2	3	4	Não importante.
1.1. A informação é reconhecida como um recurso estratégico para a empresa e de grande importância para seus clientes.						
1.2. A tecnologia da informação é vista como um dos conjuntos de recursos que trazem eficiência e						

	eficácia aos programas da empresa, e não como um fim em si mesma.					
1.3.	A decisão baseada na informação e no conhecimento predomina no ambiente da empresa, frente a outros critérios.					
1.4.	A empresa planeja de forma integrada a gestão da informação através de seu ciclo de vida (criação; armazenamento; transporte; descarte;)					
1.5.	A missão da empresa está diretamente relacionada a gestão da informação e vinculada aos planos estratégicos e operacionais.					

As questões a seguir têm por objetivo analisar o apoio gerencial da informação e investimentos realizados nesta área referente aos seus ativos.

2. Apoio ao gerenciamento da informação.		0	1	2	3	4	Não importante.
2.1.	São priorizados investimentos à tecnologia da informação segundo a importância da empresa.						
2.2.	Os ativos informacionais são gerenciados através das etapas do seu ciclo de vida, independente da mídia em que se encontram armazenadas.						
2.3.	As seguintes mídias são encontradas na sua empresa:						
2.3.1.	Documento de papel						
2.3.2.	Banco de dados						
2.3.3.	Documentos eletrônicos não documentados (incluindo correio eletrônico)						
2.3.4.	Conteúdo de páginas web						
2.3.5.	Outras mídias.						

2.4.	A gestão dos ativos de informação através de seu ciclo de vida é monitorada e avaliada.						

As questões a seguir têm por objetivo analisar se a empresa utiliza normas, políticas ou práticas para garantir melhor controle e confidencialidade de suas informações.

3. .		0	1	2	3	4	Não importante.
3.1.	Existem normas, políticas e manuais para classificar o acesso à informação (uso externo, interno).						
3.2.	Existem normas implantadas para minimizar acesso indevido às informações eletrônicas e em papel.						
3.3.	Existem rotinas especiais para proteger o acesso às informações confidenciais.						
3.4.	A empresa investe na segurança da informação, garantindo a confidencialidade de seus dados.						
3.5.	Existem contratos ativos de confidencialidade perante aos seus colaboradores, garantindo o comprometimento com o sigilo das informações.						

As perguntas a seguir terão a avaliação classificada em cinco níveis:

< 0 > - Não sei responder.

< 1 > - Não se aplica na empresa.

< 2 > - Tenho conhecimento e realmente não é utilizado ou nunca ocorreu nenhum incidente.

< 3 > - Tem breve conhecimento / talvez.

< 4 > - Sim / Se aplica / Tenho conhecimento / É utilizado / Já ocorreu este incidente.

As questões a seguir têm por objetivo analisar se a empresa tem conhecimento sobre os riscos que suas informações sofrem diariamente, bem como ter conhecimento se ela já sofreu algum incidente em cima de seu ativo.

Alguns conceitos referentes ao ciclo de vida da informação:

Criação: quando a informação é criada (seja criação/impressão de um relatório, criação de senha ou até mesmo um arquivo recebido por e-mail e salvo em seu computador).

Armazenamento: onde a informação é armazenada (qualquer arquivo armazenado em qualquer mídia, seja ela, virtual, removível, papel ou localmente em sua empresa).

Transporte: o momento que a informação é transportada (seja uma pessoa transportando um relatório até outra sala ou um simples envio de e-mail).

Descarte: quando a informação é descartada (quando é excluído o arquivo de seu computador, incinerado papéis ou até mesmo descarte físico ao lixo).

4. Gestão do ciclo de vida da informação e nível de preocupação.	0	1	2	3	4
4.1. A empresa tem uma visão clara dos riscos que cerca suas informações diariamente.					
4.2. Sua empresa já teve falhas de segurança que ocasionou vazamento de informações.					
4.3. Sua empresa já teve falhas de segurança que ocasionou roubo de informações.					
4.4. Sofreu sobre acesso não autorizado às informações.					
4.5. Sofreu com modificação ou processamento ilegal dos dados.					
4.6. Já teve problemas em que a informação é criada (Criação de senha e logo após não conseguir mais acessá-la).					
4.7. Já teve problemas no transporte da informação (Planilhas					

	de cargos e salários de funcionários visualizado apenas pela gerência, porém, outras pessoas tiveram acesso).					
4.8.	A empresa tem métodos de descarte da informação que estão de acordo com as normas de descarte e prevenção da empresa.					
4.9.	Está claro para os profissionais da empresa como funciona o descarte de informações confidenciais.					

Nas questões a seguir serão tratadas algumas ameaças encontradas na literatura. Sua empresa tem sofreu alguma delas.

5. Algumas ameaças que cerca sua empresa.		0	1	2	3	4	Não importante/ sem conhecimento
5.1.	Dano físico à mídia (notebook, pen-drive, etc.).						
5.2.	Furto de equipamentos.						
5.3.	Espionagem interna.						
5.4.	Defeito de equipamentos.						
5.5.	Acesso não autorizado às informações.						
5.6.	Processamento ilegal dos dados.						
5.7.	Cópia ilegal dos dados.						
5.8.	Defeito de *Software*.						
5.9.	Uso não autorizado de equipamentos.						

As questões a seguir serão tratadas algumas ferramentas disponíveis no mercado, seja elas pagas ou gratuitas que auxiliam na prevenção da segurança da informação em sua organização. Sua empresa tem utiliza elas.

6. Ferramentas disponíveis.	0	1	2	3	4	Não importante/ sem conhecimento
6.1. Cópias de seguranças (Backups).						
6.2. Certificado digital (criptografia).						
6.3. Biometria.						
6.4. Antivírus.						
6.5. Firewall						
6.6. Controle de tráfego de rede.						
6.7. Esteganografia (Camuflar algum arquivo dentro de outro para não mostrar seu conteúdo original. Apenas seu destino terá a chave de criptografia para visualiza-lo).						
6.8. Plano de continuidade.						
6.9. Acesso e identificação de gestão de controle.						

APÊNDICE C - INSTRUMENTO DE COLETA DE DADOS FINAL

Este questionário foi aplicado no final do estudo de caso, após a aplicação das ferramentas de segurança da informação implementadas na empresa. Trata-se de um questionário voltado a identificar as maiores dificuldades, adaptações e resistências no gerenciamento das informações com estes novos mecanismos.

O questionário será focado também nas funcionalidades das ferramentas selecionadas e os desafios que a empresa encontrou em meados este processo.

Perguntas					
1. Gerenciamento das ferramentas implantadas.	Sim	Não	Talvez	Deixe sua opinião:	Não se aplica.
a. Você teve dificuldade/problema em criar as novas senhas no novo padrão?					
b. Você teve alguma resistência sobre as regras de permissões de acesso do antivírus?					
c. Você achou interessante criptografar os dados?					
d. O novo termo de responsabilidade foi esclarecedor referente às políticas da empresa?					
e. Se você teve contato com o controle de tráfego de rede, responda: Encontrou alguma dificuldade em analisar os relatórios?					
f. Você achou trabalhoso ter que monitorar e verificar o backup uma vez por semana manualmente?					
g. Você acredita que treinamento dos funcionários possa ajudar na segurança da informação?					
2. Proteção dos dados.					
a. Você consegue perceber alguma melhoria interna com as ferramentas implantadas?					
b. Você acredita que as ferramentas implantadas darão mais segurança às informações da empresa?					

3. Resistência em implantar as ferramentas.	Deixe sua opinião das respostas abaixo:				
a. Qual das ferramentas apresentou maior dificuldade no manuseio:					
b. Em sua opinião, alguma das ferramentas implantadas não deveria ter sido aplicada?					
4. Melhorias futuras.					
a. Em sua opinião, poderia ter sido implantada mais ferramentas e mecanismos de segurança?					
5. Se você for o gestor da empresa, você acredita que todos os investimentos realizados retornarão darão retorno em longo prazo?					
6. Deixe sua opinião e seus comentários:					