UNIVERSIDADE FEDERAL DE ALAGOAS - UFAL
CAMPUS ARAPIRACA
SISTEMAS DE INFORMAÇÃO – BACHARELADO - EAD

ALEKSANDRO NUNES DO NASCIMENTO
JOSÉ FERREIRA DE LIMA FILHO

SEGURANÇA DA INFORMAÇÃO: UM CONJUNTO DE PRÁTICAS QUE PROPICIA UM AMBIENTE SEGURO, COMPETITIVO E EFICIENTE NOS NEGÓCIOS

ARAPIRACA
2019

Aleksandro Nunes do Nascimento
José Ferreira de Lima Filho

Segurança da informação: um conjunto de práticas que propicia um ambiente seguro, competitivo e eficiente nos negócios

Trabalho de Conclusão do Curso de Graduação em Sistemas de Informação, do Instituto de Computação da Universidade Federal de Alagoas, *campus* Arapiraca como requisito parcial para à obtenção do título de Bacharel em Sistemas de Informação.

Orientação: Prof. Dr. Rodolfo Carneiro Cavalcante

ARAPIRACA
2019

Aleksandro Nunes do Nascimento

José Ferreira de Lima Filho

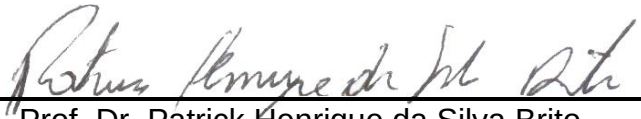
Segurança da informação: um conjunto de práticas que propicia um ambiente seguro, competitivo e eficiente nos negócios.

Trabalho de Conclusão do Curso de Graduação em Sistemas de Informação, do Instituto de Computação da Universidade Federal de Alagoas (UFAL), como requisito parcial para à obtenção do título de Bacharel em Sistemas de Informação.

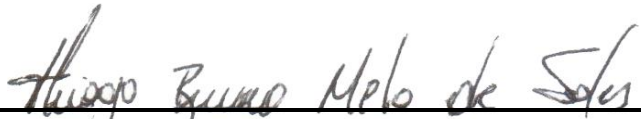
Data de Aprovação: 31 / 05 / 2019.

Banca Examinadora

Prof. Dr. Rodolfo Carneiro Cavalcante
Universidade Federal de Alagoas – UFAL
Campus Arapiraca
(Orientador)



Prof. Dr. Patrick Henrique da Silva Brito
Universidade Federal de Alagoas – UFAL
Campus Arapiraca
(Examinador)



Prof. Dr. Thiago Bruno Melo de Sales
Universidade Federal de Alagoas – UFAL
Campus Arapiraca
(Examinador)

RESUMO

A segurança da informação proporciona um ambiente favorável para as atividades cotidianas de uma empresa que faz uso de tecnologias da informação. A informação é valiosa para todos os segmentos da sociedade, bem como os avanços que a mesma nos proporcionou. Devido sua grande relevância, a aplicabilidade da segurança da informação deixou de ser algo opcional e entrou de vez na seara dos assuntos mais importantes dentre as organizações públicas ou privadas a fim de manter o funcionamento adequado de suas atividades. A segurança da informação tem sido uma questão que há muito tempo preocupa o homem, desde a antiguidade aos tempos atuais. Batalhas e guerras foram travadas onde o diferencial para a conquista ou para a derrota foi, na maioria dos casos, o nível de informação ou desinformação que um adversário possuía do outro. Com o advento da Internet, a globalização e o rápido desenvolvimento tecnológico das últimas décadas, a informação passou a ser essencial para o homem moderno. A fácil acessibilidade nessa nuvem de informações, em todo lugar e por meio de inúmeros aparelhos eletrônicos, aumentou também significativamente a preocupação em proteger certos dados, informações sigilosas que possam de alguma forma ser acessados por pessoas não autorizadas. Com isso, esta pesquisa analisou e buscou identificar as principais ferramentas, tecnologias e técnicas da segurança da informação mais utilizadas em empresas de diversos ramos de atividades. Para tanto, foram realizadas entrevistas em 20 estabelecimentos comerciais de diversos ramos de atividades na cidade de Teotônio Vilela – Alagoas, por meio de um questionário contendo 23 perguntas relacionadas ao uso da Tecnologia da Informação, sobretudo indagando proprietários e funcionários destes estabelecimentos comerciais quanto a preocupação com a segurança das informações em seus sistemas computacionais. A análise dos resultados evidenciou que apesar de todo o avanço tecnológico dos últimos tempos, a segurança da informação nessas empresas ainda está muito abaixo do desejado no contexto estudado.

Palavras-chave: Segurança da informação. Globalização. Empresas. Tecnologia.

ABSTRACT

Information security provides a favorable environment for the day-to-day activities of a company that makes use of information technology. Information is valuable to all segments of society, as well as the advances it has provided. Because of its great relevance, the applicability of information security is no longer optional, and has once again entered into the field of the most important issues among public or private organizations in order to maintain the proper functioning of their activities. Information security has long been a concern for man, from ancient times to modern times. Battles and wars were fought where the differential to conquest or defeat was, in most cases, the level of information or disinformation that one opponent possessed of the other. With the advent of the Internet, globalization and the rapid technological development of the last decades, information has become essential for modern man. The easy accessibility in this information cloud, everywhere and through numerous electronic devices, has also significantly increased the concern to protect certain data, sensitive information that can somehow be accessed by unauthorized persons. With this, this research analyzed and sought to identify the main tools, technologies and techniques of information security most used in companies of various branches of activities. For this purpose, interviews were conducted in 20 commercial establishments in various branches of activities in the city of Teotônio Vilela - Alagoas, through a questionnaire containing 23 questions related to the use of Information Technology, mainly inquiring the owners and employees of these commercial establishments regarding the concern with information security in their computer systems. The analysis of the results showed that despite all the technological advances of recent times, the information security in these companies is still much lower than desired in the studied context.

Keywords: Information security. Globalization. Companies. Technology.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

O rápido desenvolvimento científico e tecnológico após o advento da Internet transformou a maneira como as pessoas e instituições passaram a agir mediante situações que envolvem expor seus dados pessoais e financeiros, mas, sobretudo, os dados que merecem algum sigilo. Isto fez surgir alguns questionamentos em torno da segurança de informação e em como agir mediante difusão de dados pessoais em redes sociais, telefones celulares, cartões de créditos, comércio eletrônico ou em compras em lojas virtuais (CABRAL, 2015).

> Novas tecnologias e novos sistemas sempre são criados, é razoável considerar que novas vulnerabilidades sempre existirão e, portanto, novos ataques também sempre serão criados, Nakamura (2007, p. 26).

A segurança de informação ainda é considerada por algumas instituições como um elemento caro e dispensável que não traz um retorno imediato. Há muita negligência por parte dos empresários das empresas de médio e pequeno porte quando o assunto é a Segurança da Informação. Sendo essa uma realidade presente principalmente nas pequenas cidades do Nosso imenso Brasil. Estima-se que o uso de computadores em pequenas empresas ao longo dos últimos 5 anos, cresceu 30–80%, dependendo da localização e natureza do negócio (PALVIA E PALVIA, 1999).

Como resultado do rápido progresso tecnológico, essas áreas estão convergindo rapidamente e são cada vez menores as diferenças entre coleta, transporte, armazenamento e processamento de informações. Organizações com centenas de escritórios dispersos por uma extensa área geográfica podem, com um simples apertar de um botão, examinar o *status* atual de suas filiais mais remotas. À medida que cresce nossa capacidade de colher, processar e distribuir informações torna-se ainda maior a demanda por formas de processamento de informações ainda mais sofisticadas. (ANDREW S. TANENBAUM, 2003, p. 18).

> A chamada era da tecnologia trouxe-nos desenvolvimento em muitas áreas, mas principalmente na da tecnologia de informação e comunicação (TIC). diz que a informação deixou de ser um meio para alcançar outros fins, tornando-se um fim que se explica e se justifica em si mesmo. Bianchetti (2008).

É notório que os avanços que conquistamos tiveram contribuição massiva da informação, que trouxe um legado de possibilidades. Nos negócios isso não é diferente, todas as organizações precisam usufruir dos benefícios que a informação oferece. Alvin Toffler, um renomado escritor americano, no seu livro “A Terceira Onda” já alertava para o surgimento da sociedade da informação e a revolução que essa onda tecnológica causaria.

> A Primeira Onda de mudança – a revolução agrícola – levou milhares de anos para acabar. A Segunda Onda – o acesso à civilização industrial – demorou apenas uns 300 anos. Hoje a história é ainda mais acelerativa e é provável que a Terceira Onda atravesse a história e se complete em poucas décadas (TOFFLER, 1985, p. 24).

É imprescindível que se entenda o quanto é importante manter esses dados em segurança, adotar políticas de segurança que de certo modo coíbam ou ao menos dificulte a ação de criminosos virtuais, códigos maliciosos e de inúmeras ameaças que circundam no meio tecnológico.

A busca por esta proteção é o meio pelo qual pessoas e instituições se asseguram para poderem trabalhar ou simplesmente navegarem na Internet sem o medo de terem seus dados captados por agentes externos. Este receio não é sem sentido, embora muitas medidas sejam tomadas para tornar-se um ambiente mais seguro, a questão de segurança de informação será sempre mais complexa do que parece.

Assim, de acordo com Oliveira (2001), existem diferenças fundamentais na segurança tecnológica voltada para grandes corporações e para usuários domésticos. Mas em ambos os casos, a maior preocupação é a de uma invasão em seus sistemas de segurança, ou seja, um ataque externo. E é justamente essa informação que precisa ser resguardada, pois nesse ambiente convivem elementos bem e mal-intencionados. Por causa disso, diversos recursos para proteger a informação e as redes de computadores precisam ser empregados.

É através da informação que muitos negócios encontram sua base e que nos dias de hoje é algo de grande valor para as empresas. Por isso, ter consciência de que a informação precisa estar acessível apenas aos detentores dela e implantar meios que a proteja, é algo extremamente crucial para que não tenhamos problemas

quanto ao uso das tecnologias que utilizamos em nosso dia-a-dia, principalmente dentro das empresas onde estão informações sigilosas.

1.1 Justificativa

No cenário tecnológico atual, que cresce assustadoramente cada dia, nos deparamos com os mais diversos recursos e benefícios que nos são oferecidos. Porém, o que tem preocupado muito tanto para pessoas comuns quanto para empresas e instituições de um modo geral, é a segurança da informação que" trafega", é armazenada e/ou compartilhada por intermédio do uso dessas tecnologias.

Este termo tem sido utilizado por muitos especialistas da área de tecnologia da informação nas últimas décadas, devido a invasões e ataques cibernéticos que ocorrem a todo o momento em escala mundial, deixando muitas vezes prejuízos financeiros a grandes empresas; exposto a vida de milhares de pessoas por meio de roubo de perfis em redes social e, sobretudo, provocado bastantes problemas para as autoridades que pouco se tem feito para assegurar uma real proteção para esses usuários de um modo geral.

Sendo assim, esta pesquisa se justifica pela necessidade de mostrar e/ou explorar técnicas, ferramentas e práticas que propiciam um ambiente seguro, competitivo e eficiente nos negócios por intermédio da segurança da informação.

1.2 Objetivos

O objetivo principal desta pesquisa é trazer uma atenção especial para assuntos relacionados à Segurança da Informação e como ela tem sido praticada no contexto local dessa pesquisa.

1.2.1 Objetivo Geral

Apresentar as principais estratégias de segurança da informação e identificar como essa preocupação é percebida em pequenas e médias empresas do interior de Alagoas.

1.2.2 Objetivos Específicos

a) Estudo das principais práticas e do panorama em pequenas e médias empresas do interior de Alagoas.
b) Determinar as técnicas mais recentes de Segurança da Informação;
c) Identificar as ferramentas mais recentes da Segurança da Informação;
d) Verificar quais são as ferramentas e técnicas da Segurança da Informação utilizadas pelas empresas visitadas e diante dos resultados, apontar soluções simples e específicas mediante cada particularidade encontrada.

1.3 Estrutura do trabalho

Este trabalho está estruturado em seis capítulos, iniciados pela Introdução, onde apresentamos a justificativa e objetivos gerais e específicos. O capítulo 2 apresenta os trabalhos relacionados enfatizando as fontes de pesquisa utilizadas para o embasamento do conteúdo. O capítulo 3 apresenta a fundamentação teórica do trabalho onde vemos todo o contexto relacionados aos ataques, prevenções e políticas e normas de segurança da Informação.

O capítulo 4 mostra a metodologia utilizada para captura de informações mediante pesquisa de campo mediante questionário de perguntas relacionadas a utilização da segurança da informação. No capítulo 5 apresenta o estudo de caso e a análise dos dados coletados com gráficos e estatísticas. Por fim, o capítulo 6 apresenta as conclusões realizadas sobre o trabalho, explicitando a busca por contribuir para que mais e mais organizações atentem para a implantação de mecanismos de segurança para os departamentos presentes na sua organização e principalmente despertar o interesse e a atenção em relação a segurança da informação.

2 TRABALHOS RELACIONADOS

Esse trabalho foi inspirando por outras obras que retratam o uso da tecnologia de informação em médias e pequenas empresas e sobre a importância da segurança da informação, principalmente na incidência de casos de ataques e perdas de informações. Tecnologia da Informação em Pequenas Empresas: Fatores de Êxito, Restrições e Benefícios (MARCO, 2004).

Tivemos como ponto de referência a Cartilha de Segurança da Informação para a Internet, desenvolvida pelo Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança da Informação aqui no Brasil (CERT.br, 2012). O mesmo tem como objetivo a exemplificação, promoção e o incentivo para que as boas práticas sobre segurança da informação venham a ser implementadas nos mais diversos nichos da sociedade.

Outra fonte de grande estima foi o relatório previsões do McAfee Labs sobre ameaças no ano de 2017 a 2018 (McAfee LABS, 2016), onde extraímos informações e destacamos as principais ameaças do ano. Esse relatório é uma das maiores fontes em pesquisa de ameaças, inteligência contra ameaças e liderança em ideias sobre segurança cibernética.

O relatório conta com um estudo detalhado sobre vulnerabilidades e com o parecer de especialistas na área de segurança da informação que contribui para as organizações no que tange a segurança dos seus ativos. Além dos atributos mencionados, o relatório do McAfee Labs, é uma excelente referência para fonte de estudos quando se almeja aprimorar a proteção e reduzir os riscos, destacando os principais perigos que norteiam os negócios quando ligados ao meio computacional, dessa forma ele foi de grande ajuda para a implementação do presente artigo.

Esse trabalho também contou com captação de conhecimento dos grandes autores Kurose e Ross (KUROSE E ROSS, 2010). Especificamente no capítulo 8 onde aborda sobre a segurança em redes de computadores, nos auxiliando com informações para que pudéssemos explanar temas como criptografia, certificado digital, assinatura digital, *firewall* e outros temas pertinente a nossa proposta do artigo.

As normas ISO/IEC 27000 e ISO/IEC 27001 também foram instrumentos de relacionamento com nosso trabalho, nos ajudando principalmente com os princípios e normas que norteiam a vasta área da segurança da informação. O fato é que

embora as pessoas e organizações saibam o quanto é importante aplicar as recomendações de segurança nas atividades que norteiam as rotinas das organizações e nas rotinas que realizamos no dia a dia, essa área ainda carece de mais atenção. São inúmeras ameaças que norteiam as organizações e dados pessoais que podem ser acessados e destruídos.

Diante disso é importante frisar que nenhum sistema é seguro a tal ponto que seja desnecessário incrementá-lo com alguma política de segurança, isso não faz sentido nos dias de hoje. Ao contrário, é aconselhável adicionar mecanismos que possam aumentar o nível de segurança dos ativos presentes na organização a qual façamos parte, dos ativos pessoais presentes em nossas residências, qualquer que seja os dados sensíveis que nos norteiam precisam de proteção.

3 FUNDAMENTAÇÃO TEÓRICA

O trabalho busca contribuir para que as Médias e Pequenas empresas bem como a sociedade civil tenha consciência em manter seus dados seguros. Salientamos a amplitude do assunto e por isso é importante enriquecer com conhecimentos de outras obras sobre o tema, a fim de solidificar nosso entendimento sobre SI.

> No caso, informação quer dizer dados apresentados em uma forma significativa e útil para os seres humanos. Dados, ao contrário, são sequências de fatos ainda não analisados, representativos de eventos que ocorrem nas organizações ou no ambiente físico, antes de terem sido organizados e arranjados de uma forma que as pessoas possam entendê-los e usá-los. (LAUDON e LAUDON, 2010, p. 30).

Devido ao aumento significativo desses dados observou-se a necessidade de mantê-los em segurança. A partir desse ponto a segurança da informação ganhou importância e passou a ser estudada e amplamente incentivada. Embora as organizações saibam o quanto a segurança da informação é relevante para seus negócios e dos problemas iminentes quando a segurança dos ativos é negligenciada, ainda assim há muitas organizações que necessitam de fomento para que percebam afinco a importância da adoção de políticas de segurança.

É importante pautar a diferença entre hacker e cracker uma vez que iremos adentrar em conceitos técnicos sobre segurança da informação. Hacker e cracker são termos que diferentes, muito embora nós vejamos nos meios de comunicação uma grande confusão, misturando as palavras e atribuindo as mesmas aos criminosos virtuais, o que não é verdade, pois esses termos parecidos, possuem significados bastante opostos no mundo da tecnologia. Portanto, entre Hacker e Cracker existem diferenças sutis, mas que são importantes de ressaltar.

Hackers são pessoas com conhecimento em hardware e também no desenvolvimento de softwares e que se utilizam dessas habilidades para aprimorar, modificar sistemas existentes e/ou criar novos sem causar nenhum tipo de crime cibernético.

Crackers são pessoas mal-intencionadas que se utilizam de seus conhecimentos computacionais para invadir, roubar, “piratear”, de maneira que

provocam danos às suas vítimas sejam elas empresas ou pessoas. (DIGITAL, 2013).

3.1 Segurança da informação

A informação proveniente dos dados processados compõe um ativo para a organização. O ativo corresponde a algo de valor para as empresas e esse bem valioso precisa ser preservado para que nenhuma ameaça possa comprometer sua confidencialidade, integridade, disponibilidade e autenticidade. Nesse ponto destacamos que o grande objetivo da segurança da informação é garantir os requisitos necessários para proteger as informações de tal modo que esse conhecimento atenda ao negócio da organização, com isso, a segurança da informação conta com objetivos fundamentais os quais chamamos de princípios básicos que devem estar em harmonia para estabelecer níveis de segurança necessários.

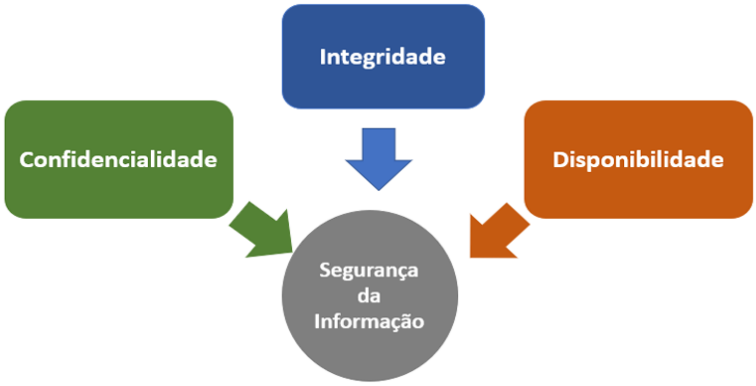
Consoante Beal (2005, p.71) ressalta que, a Segurança da Informação é o processo de proteger a informação das ameaças para garantir a sua integridade, disponibilidade e confidencialidade. Esse é o pilar básico no que concerne à segurança da informação e é a partir disso que as organizações precisam se apoiar. Vamos à definição (TECHTEM, 2018) desses princípios mencionados pela autora, mas também acrescentando outros princípios que garantem maior extensão quando aplicados em conjunto no que se refere à salvaguarda dos dados.

- **Confidencialidade** – garante que a informação somente seja acessada por pessoas autorizadas. A principal forma de garantir a confidencialidade é por meio do controle de acesso, ou seja, autenticação por senha, isso já garante que o conteúdo protegido, somente será acessado por pessoas autorizadas. Ela se dá justamente quando se impede que pessoas não autorizadas tenham acesso ao conteúdo da mensagem ou documento. Refere-se à proteção da informação contra divulgação não permitida. A perda da confidencialidade se dá quando alguém não autorizado obtém acesso a recursos e informações.
- **Integridade** – Garante que o conteúdo da mensagem não foi alterado ou violado indevidamente. Ou seja, mede a exatidão da informação e seus

métodos de modificação, manutenção e validade. Há perda de integridade quando a informação é alterada indevidamente ou quando não se pode garantir que a informação é a mais atualizada.

- **Disponibilidade** – A disponibilidade garante que a informação estará disponível para acesso no momento desejado. Diz a respeito a eficácia do sistema, ao correto funcionamento da rede para que quando a informação for necessária ela poderá ser acessada. A perda de disponibilidade se dá quando se tenta acessar uma informação e não se consegue o acesso esperado.

Figura 1 - Princípios da Segurança da Informação.



Fonte: Os autores (2018).

Vejamos na Figura 1 o modelo que representa os objetivos da segurança da informação. Alguns especialistas defendem a adição de 2 princípios à CID (Confidencialidade, Integridade e Disponibilidade), ficando com 5 princípios básicos para segurança da informação, são eles: Autenticidade e Legalidade, formando a Sigla CIDAL. C – Confidencialidade, I – Integridade, D – Disponibilidade, A – Autenticidade, L – Legalidade.

Mas seguindo os padrões internacionais sobre segurança da informação, a ISO/IEC 27002 aponta apenas 3 princípios básicos da segurança da informação: Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, não repúdio e confiabilidade, podem estar envolvidas.

Autenticidade – Garante a identidade de quem está enviando a informação, ou seja, gera o não-repúdio que se dá quando há garantia de que o emissor não

poderá se esquivar da autoria da mensagem (Irretratabilidade). Normalmente não entra como um dos pilares da segurança da informação. É através da autenticidade que se garante que a informação é proveniente da fonte anunciada, ou seja, não sofreu nenhuma alteração durante o processo.

Legalidade - o uso da tecnologia de informática e comunicação deve seguir as leis vigentes do local ou país.

Irretratabilidade ou Não repúdio – Visa garantir que o autor não negue ter criado ou assinado algum documento ou arquivo. Além dos princípios mencionados contamos também com outras técnicas que mantém a privacidade na comunicação. Vejamos as principais:

Criptografia – Segundo Pereira (2007), a criptografia é o ato de transformar a informação em uma forma aparentemente ilegível, com a finalidade de garantir a privacidade, ocultando a informação de pessoas não autorizadas. De modo mais simplificado, uma mensagem que compreendemos normalmente é criptografada, ou seja, ela é embaralhada de modo que se uma terceira pessoa tentar ler a mensagem não entenderá seu conteúdo, não sendo útil para seu propósito. Apenas o emissor e o receptor poderão acessá-la e entendê-la, evitando que um intruso consiga acessar a mensagem.

Os algoritmos de criptografia são indispensáveis para quem procura impedir o acesso ilegal a dados corporativos, uma vez que eles usam chaves de segurança que permitem verificar a validade de uma informação. Vale destacar que essa verificação pode ser feita por meio de duas técnicas: a criptografia simétrica e a criptografia assimétrica (CRYPTOID, 2017)**.**

A criptografia simétrica funciona da seguinte forma. O ciframento de uma mensagem (processo em que um conteúdo é criptografado) é baseado em 2 componentes: um algoritmo e uma chave de segurança (CRYPTOID, 2017).

A criptografia simétrica é a técnica mais antiga e mais conhecida. Uma chave secreta, que pode ser um número, uma palavra ou apenas uma sequência de letras aleatórias, é aplicada ao texto de uma mensagem para alterar o conteúdo de uma determinada maneira. Isso pode ser tão simples quanto deslocar cada letra do alfabeto em diversos locais. Desde que o remetente e o destinatário saibam a chave secreta, eles podem criptografar e descriptografar todas as mensagens que usam essa chave (Microsoft.com, 2018).

A criptografia assimétrica, também conhecida como criptografia de chave pública, é baseada em dois tipos de chaves de segurança: uma privada e a outra pública. O problema com chaves secretas está em trocá-las pela Internet ou por uma grande rede e ao mesmo tempo impedir que caiam em mãos erradas. Qualquer pessoa que conheça a chave secreta pode descriptografar a mensagem. Uma solução é a criptografia assimétrica, em que há duas chaves relacionadas - um par de chaves. Uma chave pública é disponibilizada gratuitamente a qualquer pessoa que queira enviar uma mensagem. Uma segunda chave privada é mantida em segredo, para que somente você saiba (Microsoft.com, 2018).

Qualquer mensagem (texto, arquivos binários ou documentos) que é criptografada usando a chave pública só pode ser descriptografada aplicando o mesmo algoritmo, mas usando a chave particular correspondente. Qualquer mensagem que é criptografada usando a chave privada só pode ser descriptografada usando a chave pública correspondente (Microsoft.com, 2018).

Isso significa que você não precisa se preocupar em passar as chaves públicas pela Internet (as chaves devem ser públicas). Um problema com a criptografia assimétrica, no entanto, é que ela é mais lenta do que a criptografia simétrica. Ela requer muito mais capacidade de processamento para criptografar e descriptografar o conteúdo da mensagem (Microsoft.com, 2018).

Certificado Digital – é um documento eletrônico assinado digitalmente por uma autoridade certificadora, e que contém diversos dados sobre o emissor (autoridade certificadora) e o seu titular. A função do certificado digital é a de vincular uma pessoa ou uma organização a uma chave pública.

Existem diversos tipos de certificados digitais, classificados de acordo quanto a sua aplicação ou níveis de segurança criptográfica. Com eles, é possível assinar digitalmente documentos, garantir o sigilo de seu conteúdo e proteger informações sigilosas na Internet (PEREIRA, 2018).

A ICP Brasil classifica os tipos de certificados digitais quanto duas características principais: sua aplicação e suas características de segurança. Primeiro, vamos entender cada tipo de acordo com suas aplicações práticas. Elas são três: Assinatura digital, sigilo ou confidencialidade e Carimbo do tempo. Começaremos falando sobre o mais popular, a assinatura digital (BROCARDO, 2018). A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia

hierárquica e de confiança que viabiliza a emissão de Certificados Digitais para identificação virtual do cidadão.

Ela é uma AC-Raiz, ou seja, é a primeira autoridade da cadeia de Certificação, por isso executa as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete a ela emitir, expedir, distribuir, revogar e gerenciar os Certificados das Autoridades Certificadoras de nível imediatamente subsequente ao seu (CERTISIGN).

- **Certificado tipo A – Assinatura digital:** É o tipo de certificado mais utilizado, que serve para realizar assinaturas digitais em todos os tipos de documentos. Tem como função identificar o assinante, atestar a autenticidade da operação e confirmar a integridade do documento assinado (Sandro, 2018).
- **Certificado tipo S – Sigilo/Confidencialidade:** O certificado digital de tipo S é utilizado somente para proporcionar sigilo à transação. Com ele, é possível criptografar os dados de um documento, que passa a ser acessível somente com a utilização de um certificado digital autorizado para abrir o arquivo (Sandro, 2018).
- **Certificado tipo T – Carimbo do tempo:** O certificado digital do tipo T é mais conhecido como carimbo do tempo, ou timestamp. O carimbo de tempo é um documento eletrônico emitido por uma parte confiável, que serve como evidência de que uma informação digital existia numa determinada data e hora no passado (Sandro, 2018).

3.1.1 Tipos de certificados digitais quanto à segurança

Também é possível classificar os tipos de certificado digital de acordo com seus níveis de segurança criptográfica. A ICP Brasil os agrupa em dois grupos principais: o A1, de menor segurança, e as variações A3/S3/T3, com criptografia mais complexa e, por isso, maior proteção (PEREIRA, 2018).

- **Certificados A1 -** São certificados digitais de menor segurança. Utilizam chaves de 1024 bits, geradas por um software armazenado no computador do usuário, acessível por login e senha. Têm validade de um ano. A maior

diferença prática é que eles precisam estar armazenados em um computador, portanto, não tem mobilidade. O usuário precisa estar junto do computador onde o certificado foi instalado para poder assinar digitalmente seus documentos. (Sandro, 2018).

- **Certificados A3/S3/T3 -** São certificados com níveis mais altos de criptografia de proteção das informações, e, portanto, de maior segurança. O A3 se refere aos certificados de assinatura digital, o S3 aos de sigilo e confidencialidade e o T3 aos de carimbo do tempo (PEREIRA, 2018).

Podem ter validade de até cinco anos, e utilizam chaves de 2.048 bits geradas pelo smart card ou token que armazena o certificado. A maior diferença entre os certificados de final 3 para o A1, além da maior validade e segurança, é a possibilidade de serem armazenados em dispositivos criptográficos móveis, como smartcards ou tokens. Eles também podem permanecer em uma nuvem e serem acessados pelo usuário de qualquer lugar (PEREIRA, 2018).

Embora o tema da segurança da informação já tenha sido amplamente divulgado e seja muito conhecido no meio organizacional, ainda existem muitas organizações que resistem.

3.2 Principais mecanismos de defesa

A segurança é uma corrida onde os criminosos cibernéticos estão aprimorando seus métodos com a ajuda da autoaprendizagem. Não faltam desafios no mundo da segurança da informação digital, no dia-a-dia da tecnologia presenciamos infinitas atualizações e patches em resposta a mudanças incrementais para evitar danos por parte dos criminosos virtuais.

Os grandes lançamentos de sistemas operacionais e softwares das mais variadas categorias introduzem novos recursos, mas também surgem vulnerabilidades inesperadas o que abre novas possibilidades para os cibercriminosos. Notificações e correções urgentes chegam após novas explorações serem descobertas, o que implica a necessidade da importância na segurança da informação como meio vitalício nas empresas privadas e nos órgãos públicos.

A conscientização dos colaboradores, incentivando a equipe com o desenvolvimento de atividades educativas e de conscientização que visem ao

perfeito entendimento do processo de continuidade de serviços. Além do treinamento, a conscientização pode ser feita de outras formas, como distribuição de folhetos e promoção de palestras informativas e educativas sobre possíveis acidentes e respectivos planos de recuperação. Por fim, vale salientar que um programa de educação continuada que faça com que as pessoas envolvidas se sintam como participantes ativos do programa de segurança.

Controle de Acesso - Além dos fatos expostos sobre a defesa dos ativos, destacamos também os controles de acesso aos ativos da organização, para que os mesmos tenham o mínimo de condição para sua segurança. Nesse aspecto é importante que se tenha critérios para o acesso. Os controles de acesso consistem em conceder ou negar direitos a usuários ou sistemas, definindo quais atividades poderão ser realizadas. Isso possibilita confirmar que o usuário ou algo remoto é realmente quem afirma ser. É essencial para a segurança, pois permite implementar controles, determinar quem terá acesso à informação, criar trilhas de auditoria e assegurar a legitimidade do acesso. Vejamos alguns exemplos que podem esclarecer melhor os controles de acesso:

Um funcionário de uma rede de varejo precisa de uma senha para ter acesso ao sistema de vendas, sem a senha o colaborador não conseguirá acessar o seu ambiente de trabalho. A equipe que cuida da manutenção de um data center precisa restringir o acesso ao local, o que pode ser definido por impressão digital que além de liberar o acesso, contabilizará quem entrou no centro de processamento, hora, etc. O acessa à sala de telecomunicação de um provedor de Internet pode ser liberado por cartão magnético, etc.

IDS ou Sistema de Detecção de Intrusos - é um dispositivo que gera alertas quando observa tráfegos potencialmente mal-intencionados. Segundo Kurose (2013, p.540) para detectar muitos tipos de ataques é necessário inspecionar profundamente os pacotes, analisando o cabeçalho e os dados que o pacote carrega. Função típica de um sistema de detecção de intrusos.

Exemplo do uso de um IDS é quando uma organização pretende detectar uma série de tipos de ataques, incluindo o mapeamento da rede, escaneamento de portas, escaneamento de pilhas TCP, ataques inundação de banda larga DoS, worms e vírus, ataques de vulnerabilidade de sistemas operacionais e ataques de vulnerabilidades de aplicações, etc.

VPN ou Virtual Private Network - (Rede Privada Virtual) é uma rede privada construída sobre a infraestrutura de uma rede pública, essa é uma forma de conectar dois computadores através da Internet de forma segura. Os dados trafegam criptografados garantindo a privacidade das informações.

Dentre tantos exemplos do uso de uma VPN destacamos uma empresa onde os funcionários viajam a serviço da mesma e nas localidades distantes onde se encontram necessitam acessar algum serviço nos computadores da empresa, nesse caso os funcionários utilizarão uma VPN, de modo que terão acesso aos serviços pretendidos através da Internet, mas de forma segura.

FIREWALL - Segundo Kurose (2013, p.535) um firewall é uma combinação de hardware e software que isola a rede interna de uma organização da Internet em geral, permitindo que alguns pacotes passem e bloqueando outros. Um firewall permite que o administrador de rede controle o acesso o mundo externo (Internet) e os recursos da rede interna gerenciando o fluxo de tráfego. Um exemplo simples do funcionamento do firewall são as definições dos serviços que serão permitidos ou explicitamente proibidos pelo administrador da rede, como o bloqueio dos serviços de uma rede social ou streaming de vídeo.

HONEYPOT - Segundo Assunção (2008) honeypot é uma ferramenta ou sistema criado com objetivo de enganar um atacante e fazê-lo pensar que conseguiu invadir o sistema, quando na realidade, ele está em um ambiente simulado, tendo todos os seus passos vigiados.

Exemplo do uso da técnica de honeypot é quando uma organização pretende elaborar um estudo detalhado com as informações capturadas dos atacantes, a partir dessas informações novas alternativas e técnicas poderão ser criadas contra futuros ataques.

3.3 Principais tipos de ataques

3.3.1 Ameaças internas

Quando pensamos em ameaças à segurança da informação de uma empresa imaginamos que essas ameaças se originam de fora, contudo no âmago interno da empresa situações que podem causar contratempos no que se refere à segurança da informação. Os funcionários podem ser uma ameaça, sejam por causa do acesso

às informações importantes, insatisfação com a remuneração ou por uma relação conturbada com os superiores, desleixo, ingenuidade, enfim.

> Pesquisas concluíram que a falta de conhecimento dos usuários é a maior causa isolada de falhas na segurança de redes. Muitos funcionários esquecem a senha para acessar o sistema de computadores, ou permitem que colegas a utilizem, o que compromete o sistema todo. Intrusos mal-intencionados em busca de acesso ao sistema podem enganar os funcionários fingindo serem membros legítimos da empresa; assim, conseguem fazer com que revelem sua senha. Essa prática é denominada engenharia social. (LAUDON, 2010, p. 226).

Ainda no que se refere às ameaças internas um assunto de grande relevância é a engenharia social como citado por Laudon, o atacante usa o poder de persuasão de modo a envolver a vítima e com isso consegue informações importantes para que o mesmo possa dar continuidade nos planos de ataque. Um ponto crucial na implantação de políticas de segurança de informação é o envolvimento dos colaboradores como parte dessa política, sem eles a implantação de políticas de segurança será propensa a falhas.

> A medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tonando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltaram cada vez mais para a exploração do elemento humano (MITNICK E SIMON, 2003, p. 4).

Diante do que foi citado fica ainda mais evidente que treinar os funcionários e colaboradores para que eles tomem consciência da relevância dos cuidados com informação na continuidade dos negócios, e, também, para o sucesso da organização nos seus objetivos estratégicos é uma tarefa tão importante quanto investir massivamente em tecnologia de ponta na segurança. Contemplar a equipe que compõe a organização com treinamentos, palestras e workshop integram os funcionários como o principal componente na política de segurança que se deseja implantar, afinal de contas o ser humano é o elo mais fraco na composição dos mecanismos de segurança.

3.3.2 Ameaças externas

No âmbito das ameaças externas existem uma vasta quantidade de softwares maliciosos e técnicas empregadas com a intenção de acessar dados sem autorização, deixá-los indisponíveis, alterar seu conteúdo, deletá-los, bem como outras ações que prejudiquem a imagem da organização para seus clientes, fornecedores e a sociedade em geral. Quando estamos analisando as ameaças externas além da preparação do quadro de funcionários, contamos também com recursos tecnológicos que auxiliam na proteção do ativo organizacional, atribuímos que esses recursos são recursos físicos e lógicos.

Os recursos físicos são os que de forma direta conseguimos tocar, ver sua configuração e termos uma noção clara do seu funcionamento, exemplo a respeito desse atributo seriam as portas com identificação digital, os nobreaks e até mesmo os seguranças que ficam fiscalizando os departamentos aos arredores da empresa. No lógico temos os softwares que analisam os tráfegos de dados pela rede, que bloqueiam acesso suspeito, políticas de backups, etc.

Pontuaremos as ameaças externas mais comuns descritas na Cartilha de Segurança para Internet do CERT.br, contundo, em virtude dos avanços da tecnologia, novas técnicas vão surgindo o que exige que as organizações orientadas pelos especialistas em segurança ou empresas prestadoras de serviços de segurança estejam atentas ao surgimento de novas ameaças.

Ressaltamos que a cartilha de segurança da informação elaborada pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), que é um dos serviços prestados para a comunidade da Internet do Brasil pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), o braço executivo do Comitê Gestor da Internet no Brasil (CGI.br). A Cartilha de Segurança para Internet e um documento com recomendações e dicas sobre como o usuário e as organizações devem se comportar para aumentar a sua segurança e se proteger de possíveis ameaças. Vamos as definições:

- **Exploração de vulnerabilidades**: definiremos vulnerabilidades como uma brecha que quando explorada por um agente pode comprometer a segurança da organização. Comitê Gestor da Internet no Brasil destaca

que vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.

- **Varredura em Redes**: segundo o Comitê Gestor da Internet no Brasil a varredura em redes é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Através dessas informações é possível que o agente infrinja os princípios de segurança da informação.
- **Falsificação de e-mail**: ainda segundo o Comitê Gestor da Internet no Brasil em sua cartilha da segurança da informação a falsificação de e-mail, ou e-mail spoofing, é uma técnica que consiste em alterar campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.
- **Interceptação de tráfego**: essa técnica conhecida como "*sniffing"* analisa os dados que são trafegados na rede com o uso de softwares. Essa técnica pode ser usada tanto para fins legais como também para ilegais como os praticados pelos crackers.
- **Força bruta**: Um ataque de força bruta consiste em adivinhar, por tentativa de erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário.
- **Desfiguração de página**: conhecido tecnicamente por "*defacement"* essa ação altera todo o conteúdo do site. Na realidade essa técnica picha todo o site, furta senhas de acesso à interface web usadas para administração remota.
- **Negação de Serviço**: talvez o mais conhecido pelo público, essa técnica visa sobrecarregar um serviço na rede. Todos os serviços oferecidos pelos sites e servidores espalhados pelo mundo têm um limite de conexões que ele pode atender por vez, acontece que a negação de serviço (DoS) utiliza um computador para fazer uma grande quantidade de requisições ao site de modo que ele não consiga atender a todas as solicitações e para de funcionar. E para aperfeiçoar ainda mais essa técnica contamos hoje em dia com o DDoS (Distributed Denial of Service) que consiste em utilizar

milhares de computadores autônomos, muitas vezes sem o conhecimento do proprietário para realizar a sobrecarga em um serviço remoto.

3.3.3 Tipos de códigos maliciosos

No que se referem aos códigos maliciosos, eles são projetados para executar ações danosas e atividades maliciosas em um computador. Há uma grande variedade de malwares, alguns conhecidos, outros vão surgindo, e assim, exige que devamos estar atentos para as novas ameaças que circundam no meio virtual.

- **Vírus**: é um programa ou parte de um programa malicioso que se propaga através da interação do usuário com esse programa.
- **Worm**: é um programa malicioso que consegue se propagar automaticamente sem a necessidade da intervenção do usuário.
- **Bot e botnet**: é um programa malicioso que uma vez instalado em um determinado computador mantém comunicação com o invasor remotamente. Ele se propaga semelhante ao worm, ou seja, automaticamente.
- **Spyware**: é um software malicioso desenvolvido para monitorar as atividades do computador e enviar as informações coletadas para o invasor.
- **Backdoor**: é um software malicioso que abre brechas e possibilita o retorno do invasor por essas brechas.
- **Cavalo de Troia**: conhecido popularmente como (*Trojan*) é um código malicioso que além de executar as funções projetadas, aparentemente um programa inofensivo e até útil para o usuário, ele consegue executar outras funções maliciosas sem o conhecimento do mesmo.
- **Rootkit**: é um código que permite esconder e permitir a presença de um invasor ou outro código malicioso em um computador.

Na Figura 2, temos uma tabela com um resumo dos códigos maliciosos, de como eles podem ser obtidos e as particularidades de cada um. Complementando a lista dos códigos maliciosos temos o *ransomware***,** que é uma espécie de software mal-intencionado que os criminosos instalam no computador ou servidor da vítima

sem seu consentimento. O ransomware dá aos criminosos a possibilidade de bloquear o computador de um local remoto, depois, ele apresenta uma janela pop-up com um aviso de que seu computador está bloqueado e você não poderá acessá-lo, a menos que pague.

Figura 2 - Resumo comparativo entre os códigos maliciosos.

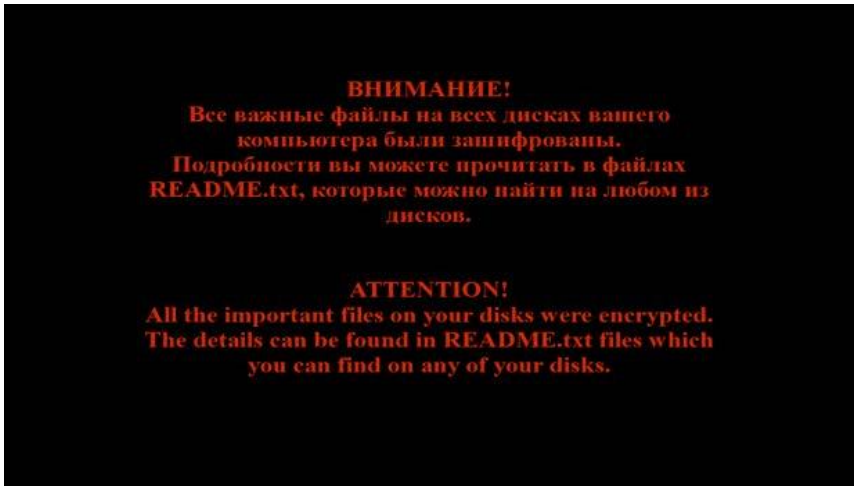
Códigos Maliciosos	VÍRUS	WORM	BOT	TROJAN	SPAWARE	BACKDOOR	ROOTKIT
Como é obtido:							
Recebido automaticamente pela rede		✓	✓				
Recebido por e-mail	✓	✓	✓	✓	✓		
Baixados de sites na internet	✓	✓	✓	✓	✓		
Compartilhamento de arquivos	✓	✓	✓	✓	✓		
Uso de mídias removíveis infectadas	✓	✓	✓	✓	✓		
Redes sociais	✓	✓	✓	✓	✓		
Mensagens instantâneas	✓	✓	✓	✓	✓		
Inserido por um invasor		✓	✓	✓	✓	✓	✓
Ação de outro código malicioso		✓	✓	✓	✓	✓	✓
Como ocorre a instalação:							
Execução de um arquivo infectado	✓						
Execução explícita do código malicioso		✓	✓	✓	✓		
Via execução de outro código malicioso						✓	✓
Exploração de vulnerabilidades		✓	✓			✓	✓
Como se propaga:							
Insere cópia de si próprio em arquivos	✓						
Envia cópia de si próprio automaticamente pela rede		✓	✓				
Envia cópia de si próprio automaticamente por e-mail		✓	✓				
Não se propaga				✓	✓	✓	✓
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✓			✓			✓
Consome grande quantidade de recursos		✓	✓				
Furta informações sensíveis			✓	✓	✓		
Instala outros códigos maliciosos		✓	✓	✓			✓
Possibilita o retorno do invasor						✓	✓
Envia Spam e Phishing			✓				
Desfere ataques na Internet		✓	✓				
Procura se manter escondido	✓				✓	✓	✓

Fonte: CERT.br (2012).

Na Figura 3, mostra uma tela com o aviso de um ataque de ransomware com uma mensagem informando ao usuário que o seu computador foi bloqueado e que os dados não podem ser acessados.

É comum encontrarmos órgãos públicos sem o mínimo de segurança com os seus dados, ainda existe esse desleixo em vários setores da sociedade, para termos uma ideia várias prefeituras, órgãos estaduais e até federais tiveram seus serviços suspensos devido ao ransomware que é um tipo de malware que sequestra o computador da vítima e cobra um valor em dinheiro pelo resgate, falamos sobre ele no parágrafo anterior, geralmente o agente que disseminou o ransomware usa moeda virtual bitcoin, que torna quase impossível o rastreamento do criminoso, esse tipo de vírus age codificando os dados do sistema operacional de forma que o usuário não consegue ter acesso.

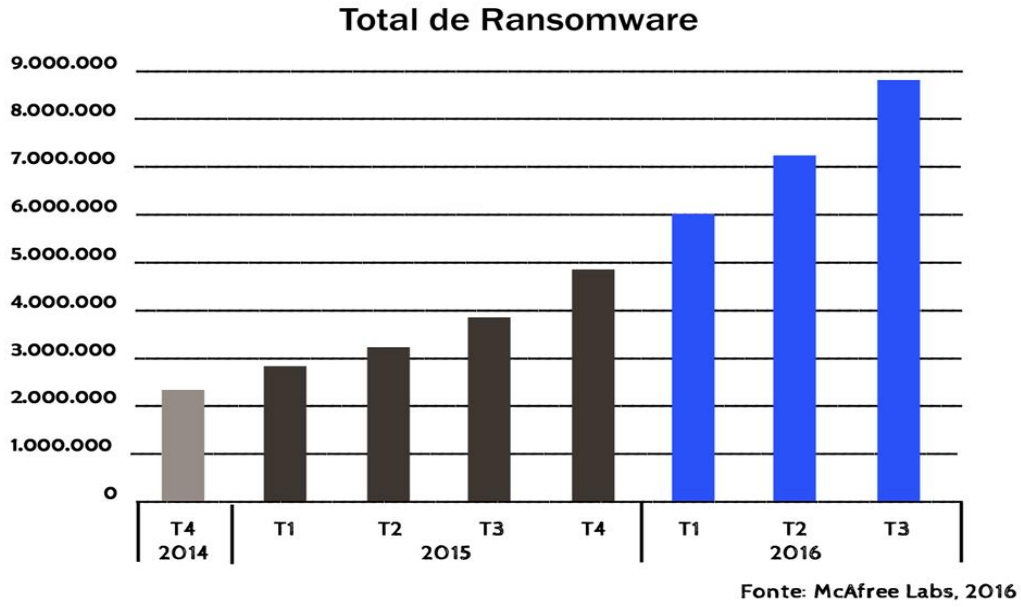
Figura 3 - Aviso de que o computador está bloqueado.



Fonte: Relatório McAfee Labs - Previsões sobre Ameaças em 2017 (2017).

A Figura 4, mostra o aumento dos números de ataques de Ransomware. Segundo o relatório de previsões sobre ameaças de 2017 da McAfee Labs, o número de ataques de ransomware subiu gradativamente nos anos subsequentes ao ano de 2014.

Figura 4 - Quantidade total de Ransomware.



Fonte: Relatório da McAfee Labs - Previsões sobre Ameaças em 2017 (2017).

Esses são os problemas de maiores proporções que não podem ser resolvidos por atualizações ou patches de software, para resolver esses problemas é preciso muita pesquisa de base, investimento pesado em tempo e trabalho de desenvolvimento e um foco sustentado, frequentemente por vários participantes do setor atuando conjuntamente. Durante os últimos anos, o uso rapidamente crescente de serviços na nuvem, a diminuição da distância entre redes internas e externas, fluxo incrível de dados e de novos dispositivos conectados desafiaram os métodos tradicionais de proteção de tudo que seja digital, exigindo maior atuação no âmbito da segurança da informação.

De acordo com Mitnick e Simon (2003) uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio da melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável.

Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada ao sistema e a realizar periodicamente a instalação das correções de segurança. Mesmo assim esses indivíduos estarão vulneráveis, a organização estará vulnerável, isso porque a segurança da informação é uma atividade constante, necessita ser estudada todos os dias, precisa estar em alerta aos avanços cotidianos.

3.4 Políticas de segurança

No que tange as políticas de segurança da informação, as organizações vêm buscando diminuir os riscos inerentes ao processamento de informações adotando boas práticas de gerenciamento, essas práticas de gerenciamentos denominamos de políticas de segurança de informação. Mas o que vem a ser uma política de segurança? Para Dantas (2001), políticas de segurança são normas organizacionais de cumprimento obrigatório, que tentam padronizar o comportamento de todos que tem algo a ver com a organização, os chamados stakeholders. Ou seja, gestores, colaboradores, clientes, fornecedores, visitas, etc.

Para Fontes e Araújo (2008), se a organização quer assegurar que determinado ativo tenha um certo controle para que sua segurança seja mantida, ela constrói uma política de segurança e assim todos agirão conforme os procedimentos daquela política. Por exemplo: várias empresas o uso do crachá é obrigatório, outras organizações proíbem veementemente o uso de redes sociais em horário comercial, outras até proíbem o uso delas independente do horário. Essas normas além de padronizar a estrutura funcional estabelece uma finalidade acerca de um determinado comportamento.

Segundo Freitas e Araújo (2008), a política de segurança da informação de uma organização consiste em um documento elaborado contendo uma lista de obrigações direcionadas aos colaboradores e que é amplamente divulgada na instituição. Vale ressaltar que esse documento é atualizado sempre que houver necessidade de modo que mantenha a organização em níveis de segurança aceitáveis.

Mas para que uma organização possa elaborar esse documento é preciso saber o que ela precisa manter em segurança, sim, porque nem toda informação tem a mesma criticidade no que se refere a salvaguarda dos dados. Por exemplo: embora uma lista de compras do almoxarifado seja algo peculiar de uma empresa não teria tanta gravidade quanto a um documento contendo um projeto de expansão se ambos fossem acessados por alguém não autorizado.

Perceba que ambos são informações da organização, mas com níveis de criticidade diferentes, o primeiro é importante e é uma informação interna, que deve ter sua disponibilidade negada ao meio externo, mas caso ocorra o acesso não autorizado não acarretaria em algo extremamente danoso à instituição. No segundo exemplo, o documento de expansão representa algo do âmbito estratégico da organização, caso esse documento venha a ser acessado no meio externo seria extremamente nocivo à organização, visto que isso poderia ser copiado por um concorrente ou até mesmo ser sabotado por um concorrente.

Portanto, antes que a política de segurança da informação seja elaborada é importante saber quais ativos pertencem à organização, Ferreira (2017). O grau de criticidade de cada ativo, descobrir quais as vulnerabilidades inerentes à instituição e as respectivas ameaças. Após esse levantamento a organização terá condições de elaborar sua política de segurança da informação.

3.5 Instituições padronizadoras de normas de segurança

As instituições padronizadoras de normas de segurança da informação foram criadas para fornecer as melhores práticas, diretrizes e princípios gerais para a implementação de sua gestão para qualquer organização. Com o crescimento da utilização da informática pelas organizações, na década de 80 e 90, o Departamento de Defesa (DoD – Department of Defense), disponibilizou uma série de publicações com padrões e orientações sobre segurança da informação que ficaram conhecidas como “Rainbow Series” ou “Rainbow Books”.

No Reino Unido na década de 90 surgiram as normas BS (British Standard). No contexto da segurança da informação, em 95 foi publicada a BS7799 que anos mais tarde iria se transformar na ISO 27002 e 27001. Inspirada no “Orange Book” foi publicada a norma ISO 15408, que trata do desenvolvimento de software seguro e publicada a RFC 2196, do IETF, que é um guia para desenvolvimento de políticas de segurança de computador e procedimentos para sites que têm seus sistemas na Internet.

Como podemos concluir existem várias instituições reconhecidas que produzem padrões na área de segurança da informação, segue as mais importantes:

- ISO – International Standardization Organization;
- IEC – International Electrotechnical Comission;
- ABNT – Associação Brasileira de Normas Técnicas;
- IETF – Internet Engineering Task Force;
- IEEE – Institute of Electrical and Electronics Engineers.

4 METODOLOGIA

Através de um estudo de caso realizado em 20 estabelecimentos comerciais por meio de um questionário de pesquisa contendo 23 perguntas relacionadas ao uso de sistemas computacionais e as preocupações com a segurança das informações. O objetivo deste questionário foi analisar as diversas situações cotidianas no uso dos sistemas computacionais quando utilizados. Nos casos que não são informatizados, o objetivo foi de analisar fragilidade quanto ao armazenamento de informações importantes do estabelecimento, tais como, contas a pagar e a receber, estoques, controle de produtos e clientes.

Utilizamos a pesquisa de campo quantitativa descritiva para obter o objetivo desejado e assim, coletar dados através de cada entrevistado, utilizando um questionário com perguntas específicas a respeito do uso da segurança da informação.

4.1 Objetivos da entrevista

A pesquisa foi realizada em vinte empresas de pequeno e médio porte de vários segmentos de negócios na cidade de Teotônio Vilela – Alagoas, a respeito do uso da segurança da informação em seus respectivos estabelecimentos a partir de uma entrevista individual, com o objetivo de coletar, analisar e interpretar os fatos e fenômenos que ocorrem dentro de seus nichos, cenários e ambientes naturais de vivência. E, através de cada informação obtida, chegamos ao resultado fundamentado em nosso tema proposto neste trabalho.

4.2 Design da entrevista

Abaixo nas Figuras 5 e 6, veremos as perguntas do questionário utilizado para a pesquisa de campo realizada em cada um dos estabelecimentos comerciais entrevistados. As perguntas foram direcionadas tanto aos proprietários, como para os funcionários indicados por estes. Através do questionário, fizemos um levantamento a respeito do conhecimento e/ou utilização da segurança da informação por parte de algumas empresas locais e assim obtivemos um resultado

específico de como lidam com o assunto, sobretudo, apuramos a realidade presente mediante seus recursos, políticas e práticas implantadas.

Figura 5 - Questionário sobre o uso da segurança da informação em pequenas e médias empresas.

Universidade Federal de Alagoas - UFAL
Instituto de Computação – IC
Curso: Bacharelado em Sistemas de Informação
Trabalho de Conclusão de Curso
Orientador: Professor Dr. Rodolfo Cavalcante
Alunos: **Aleksandro Nunes do Nascimento**
José Ferreira de Lima Filho

Pesquisa: Estudo de caso sobre o uso da segurança da informação em pequenas e médias empresas:

Empresa:_____Cidade:Teotônio Vilela -AL
Entrevistado(a):_____Data:_____

1. Quantos funcionários a sua empresa possui?

2. Qual nível de informatização em sua empresa?
   a. Totalmente Informatizada
   b. Parcialmente Informatizada
   c. Não está informatizada

3. Caso seja totalmente ou parcialmente informatizada, qual o impacto que a parada parcial ou total do sistema tem sobre os aspectos financeiros da empresa?
   a. Prejudica o faturamento
   b. Não Prejudica o Faturamento

   - ***As perguntas a seguir se aplicam ao caso de empresas totalmente informatizadas ou parcialmente informatizadas.***

4. Qual componente do sistema computacional assume maior importância para a empresa?

5. Existe algum mecanismo de proteção a este(s) componente(s)? Sim ( ) Não ( )
   Se a resposta for sim, quais?
   a. Proteção Física
   b. Proteção Lógica

6. No caso de existência de uma rede de computadores, quantos pontos de conexão com a internet e/ou com outras existem?

7. Existe algum mecanismo de proteção a esta rede? Sim ( ) Não ( )
   a. Proteção Física
   b. Proteção Lógica

8. Qual (is) sistema (s) operacional (is) é (são) utilizado (s)?

   a. Windows. Qual versão?_____

b. Linux. Qual Versão?_____
c. Android
d. IOS

9. O(s) sistema(s) operacional(is) é (são) atualizado(s)? Sim ( ) Não ( )
   Se a resposta anterior foi sim, qual a frequência? Diária( ), semanal( ) ou mensal( )?

10. O Acesso aos componentes do sistema computacional se dá por meio de senhas?
    Sim ( ) Não ( )

11. Se sim, existe uma política de troca de senhas? Sim ( ) Não ( )
    Se a resposta anterior foi sim, qual a frequência? Diária( ), semanal( ) ou mensal( )?

12. Existe alguma política para concessão e/ou compartilhamento de senhas?

13. São realizadas cópias das informações armazenadas no sistema computacional?

14. Se sim, qual a frequência? Diária( ), mensal( ) ou semanal( )?

15. Qual dispositivo é utilizado para a realização destas cópias?

16. Este dispositivo serve para outras finalidades?

17. Já ocorreram perdas de informações? Sim ( ) Não ( )

18. Se sim, como ocorreu este evento?

19. Quais foram os impactos?

    a. Houve prejuízo financeiro para a empresa? Você conseguiria estimar este prejuízo em termos percentuais (Ex: Houve uma perda de x% do faturamento no mês de ocorrência).
    b. Houve perdas de informações dos clientes
    c. Houve perda do cadastro de produtos
    d. Houve perda no cadastro de fornecedores

20. Você já ouviu falar em Política de Segurança? Sim ( ) Não ( )

21. Existe alguma norma que orienta os funcionários em suas atitudes para o caso de falha(s) acidental ou intencional no sistema computacional?

22. Existe alguma regra que regulamenta o acesso às redes sociais e outros meios de entretenimento na internet a partir dos computadores da empresa?

23. Diante desse tema, você acha importante investir em segurança da informação em sua empresa?

Fonte: Dados da pesquisa (2018).

A pesquisa semiestruturada por meio de entrevistas/questionário, visou também saber a respeito de como cada entrevistado lida com a segurança de suas informações e assim configurou o resultado mediante um pequeno levantamento quanto ao uso da tecnologia da informação, levando em consideração os que a utilizam; como lidam e a importância dada no que se refere à segurança da informação.

Foi utilizado um questionário padrão para todos os entrevistados independente do seguimento, porte e/ou tamanho da empresa; pois, os critérios para seleção das empresas escolhidas nesta entrevista foram: Empresas particulares, com 2 a 30 funcionários e que oferecem serviços e atividades de relevância no comércio local. Neste caso, dentre os entrevistamos estavam: Supermercados, Farmácias, Lojas de Materiais de Construção, Lojas de Confecções e Calçados, Artigos para Festas e Importados, Loja de Fotografias, Granjas e algumas mercearias de porte pequeno; ambos na cidade de Teotônio Vilela – AL.

5 ESTUDO DE CASO SOBRE SEGURANÇA DA INFORMAÇÃO E AS PRINCIPAIS PRÁTICAS E O PANORAMA EM PEQUENAS E MÉDIAS EMPRESAS DO INTERIOR DE ALAGOAS

5.1 Análise dos dados

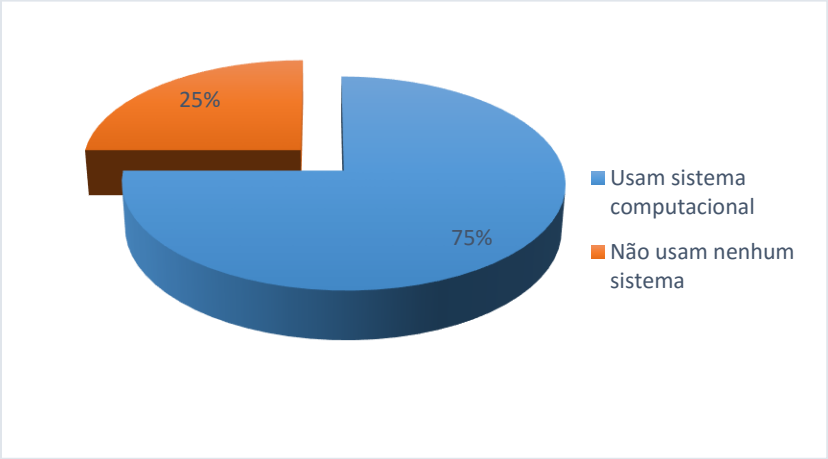
Os resultados obtidos nesta pesquisa revelam o quanto é importante se investir em segurança da informação. Apesar de termos encontrados ainda muitas empresas que nem sequer utilizam algum sistema computacional adotando o velho e conhecido método do “caderninho de anotações”; sendo assim, não acham necessário o investimento em tecnologia e por isso, preferem colocar em risco a segurança e o controle de seus negócios.

> Diante dessa realidade encontrada, nos fez lembrar uma frase dita por Brad Smith (Vice-Presidente executivo e conselheiro geral da Microsoft) certa vez numa entrevista; “As pessoas só irão utilizar tecnologias de informação se conseguirem confiar nelas”.

Deparamo-nos com uma boa parte de empresas que já possuem uma preocupação e/ou atenção específica quanto à segurança da informação e por que não dizer “política de segurança”, mesmo que de uma maneira simples e sem muito investimento em equipamentos, pessoas e serviços especializados. A respeito do controle de acesso a(s) máquina(s) dos estabelecimentos, vimos que não se costumam troca senhas periodicamente, mas, existiram casos que a senha utilizada é a mesma desde a implantação do sistema ou informatização da empresa; chegando a ter senhas de 1 até 5 anos sem nunca terem sido alteradas.

Todos os entrevistados que utilizam sistemas computacionais acham importante investir em segurança da informação e alguns até foram motivados a investir mais um pouco mediante terem respondido essa pesquisa. Vejamos o resultado e a análise da pesquisa realizada, seguida de sugestões de melhorias em alguns pontos que consideramos primordiais para garantir a segurança das informações:

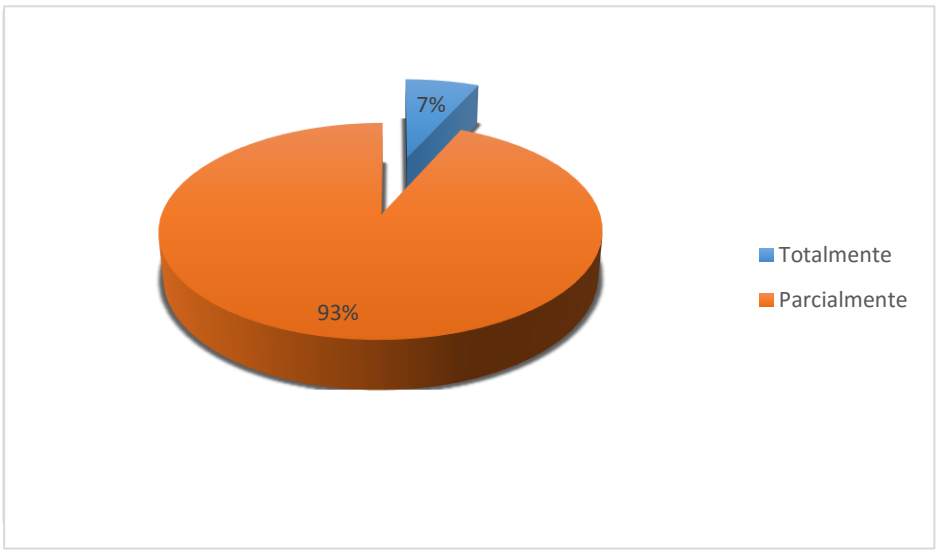
Figura 6 - Uso de Sistemas Computacionais



Fonte: Dados da pesquisa (2018).

A Figura 7 mostra que 15 dos 20 entrevistados usam sistema computacional, tais como Computadores ou Notebook com Softwares de controle de estoque, controle de vendas, cadastro de fornecedores e clientes; e que apenas 5 deles não usam sequer um computador para guardar as informações necessárias e importantes, pois, utilizam ainda o método do “caderninho de anotações”.

Figura 7 - Nível de informatização



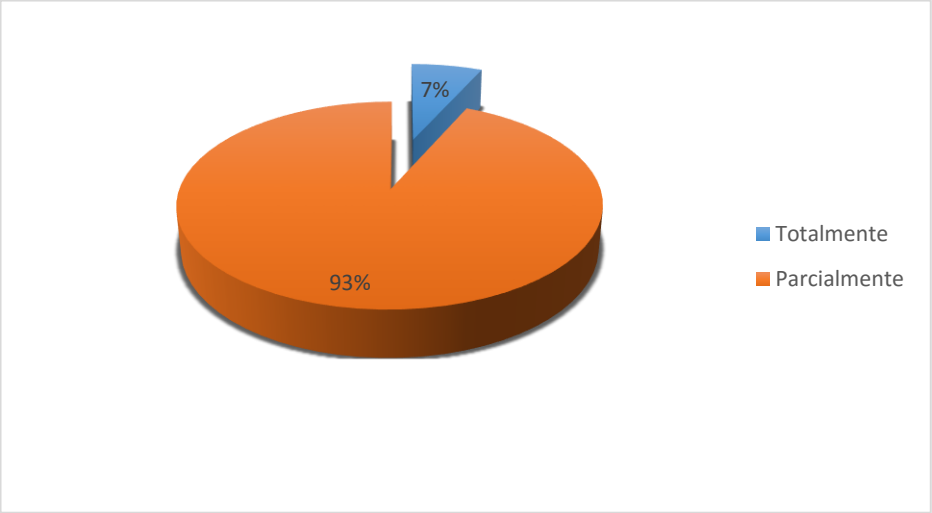
Fonte: Dados da pesquisa (2018).

Na Figura 8, mostra que 15 entrevistados são informatizados, sendo que apenas 1 é totalmente (onde todos os processos da empresa são informatizados,

salvos em um banco de dados armazenado em um sistema computacional gerido por um ou mais softwares específicos) e 14 parcialmente informatizados (onde apenas alguma informação é gravada através de um software de controle de estoque e que não utilizam para cadastro de clientes ou fornecedores).

Compreendemos que a informática se tornou uma grande aliada para empresas e indivíduos no que se diz respeito a ferramentas e recursos tecnológicos que auxiliam nas atividades cotidianas. Através da informatização muitas empresas adquiriram melhorias em seus comércios ao longo do tempo, e assim, consequentemente obtiveram maior êxito em seus negócios devido ao uso das tecnologias existentes, tais como, os sistemas de informação adequados, que garantem a qualidade e o controle em todos os processos que envolvem as atividades das empresas informatizadas.

Figura 8 - Percentual das empresas que fazem backup



Fonte: Dados da pesquisa (2018).

Na Figura 9, apresentamos o resultado das empresas que se utilizam dos backups como meio de salvaguardar seus dados. Através da entrevista, podemos detectar falhas na utilização dos sistemas computacionais devido a negligência e/ou falta de conhecimento por parte dos empresários e /ou funcionários responsáveis pelo manuseio dos mesmos.

Quando perguntados se realizavam alguma forma de backup para proteger suas informações em local seguro; a maioria foi positiva quanto à resposta: 60% dos entrevistados realizam o backup diariamente; 7% fazem mensalmente e 33%

disseram não realizar backups; para esses que não utilizam a prática de salvar seus dados; orientamos à o fazer sempre e diariamente, pois, explicamos os perigos de perdas de informações importantes, como também, a possível geração de prejuízo financeiro mediante a perda do controle de contas a receber ou simplesmente a perda do banco de dados de informações de produtos cadastrados e etc.

Algo muito comum foi encontrarmos computadores desktops de uso doméstico sendo utilizados como “servidor” e sem nenhuma proteção seja física ou lógica; sistemas operacionais totalmente desprovidos de atualizações de segurança e até mesmo sem suporte algum há anos; ausência de programas de proteção tais como antivírus e o próprio firewall do sistema, quando não atualizados, desativados; em todos os casos, o Sistema operacional utilizado foi o Windows 7.

O fato de senhas de acesso serem compartilhadas foi uma ação comum encontrada e que orientamos a não permitir isso, pois podem gerar problemas quanto ao controle e a identificação de possíveis erros cometidos por usuários e funcionários. Encontramos também o uso do mesmo equipamento que contém um sistema computacional que guarda o banco de dados da empresa (em alguns casos o mesmo computador tido como servidor) sendo utilizado para entretenimento e redes sociais tanto por parte dos proprietários quanto de funcionários que também utilizam para pesquisas e outros acessos à Internet.

Sendo assim, orientamos sobre a necessidade de se ter um equipamento exclusivo para o servidor e que o correto seria a instalação de um ou mais terminais para serem utilizados pelos funcionários de maneira que só tivesse acesso aos sistemas e/ou softwares relacionados ao trabalho. Falamos aqui sobre as possíveis invasões ou contaminações por vírus ou pragas da grande rede através de acesso a páginas não seguras ou algo parecido.

A falta de informação ou conhecimento, a falta de recursos ou o simples fato de não ter noção dos possíveis prejuízos causados pelo uso errado dos sistemas computacionais, são fatores que interferem diretamente na questão da prevenção e na tomada de decisão referente a ações ligadas a segurança da informação.

Após as entrevistas, que envolveram tanto proprietários como funcionários indicados pelos estabelecimentos, oferecemos um feedback técnico a respeito de cada particularidade e de como poderia ser resolvido os problemas encontrados mediante investimentos, treinamentos e consultorias em cada caso.

Houve um comprometimento por parte de alguns empresários em investir em treinamentos para seus funcionários especificamente os que lidam com a parte de informatização da empresa; e ao final apresentamos um checklist aonde apontamos possíveis causas de ataques, invasões, perdas de informações e sobretudo prejuízos que poderiam vir a ocorrer naquela empresa devido a ausência de uma “política simples” de segurança da informação respectivamente.

Exemplo: checklist básico:

1 - Alterar senhas de acesso periodicamente e não compartilhar;
2 - Utilizar e manter atualizados os Antivírus;
3 - Sempre realizar backups;
4 - Treinar os funcionários;
5 - Utilizar Nobreaks.

6 CONCLUSÃO

Diante do que foi estudado chegamos à conclusão que a segurança da informação é um modelo de gestão que garante maior segurança dos ativos organizacionais. Ter condições necessárias para que esses ativos estejam bem protegidos, de modo a garantir a continuidade dos negócios e, consequentemente, possibilitar o crescimento da entidade. Podemos compreender que algumas organizações embora tenham ciência da importância da segurança para seus ativos, ainda não dispõe de políticas adequadas.

O objetivo retratado nesta monografia busca contribuir para que mais e mais organizações atentem para a implantação de mecanismos de segurança para os departamentos presentes na organização, sobretudo que a segurança da informação esteja sempre presente e alinhada aos objetivos estratégicos da empresa ou do órgão governamental.

É importante reiterar que os dados, informações, o conhecimento advindo do estudo das informações organizacionais, os meios de comunicação, hardware e software, são todos ativos, ou seja, algo de valor que precisa ser mantido em segurança para que as informações não sejam acessadas por quem não tem autorização para tanto. As pessoas que compõe o quadro funcional também fazem parte da política de segurança e que precisam estar preparadas para as ameaças que objetivam destruir ou de algum modo impedir que os ativos funcionem, deixando de atender aos anseios da empresa.

Por fim, foi apresentando as principais ameaças que as organizações devem conhecer para se proteger, e a partir disso montar a política que atenda aos objetivos que a organização estabeleceu. Vivemos na era do conhecimento e o conhecimento é o diferencial competitivo e estratégico que emana no crescimento que tanto buscamos. Um ambiente organizacional seguro, que disponha de meios que tonem essa proteção real possibilitar níveis de crescimento, satisfação do cliente e, sobretudo, uma imagem organizacional que passe credibilidade.

Consumidores e empresas precisam de privacidade e segurança, conforme o crescimento e a expansão da tecnologia e das ferramentas digitais que permeiam cada vez mais no nosso cotidiano cresce também a necessidade da segurança da informação.

Futuramente o nosso intuito é voltar em cada empresa entrevistada e ver o que mudou após a implantação das políticas de segurança sugeridas e realizar outra pesquisa acompanhada de uma consultoria específica para melhorias em cada seguimento de negócios presentes no comércio local de nossa cidade.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO / IEC 27002:** tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

BEAL, Adriana. **Segurança da informação.** São Paulo: Atlas, 2005.

CERT. br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de segurança para internet**: versão 4.0. São Paulo: CERT.br, 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf Acesso em: 15 jan. 2018.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Cartilha de segurança para internet**. Disponível em: https://cartilha.cert.br/sobre/. Acesso em: 20 out. 2018.

CERTISIGN. **O que é certificado digital.** Disponível: https://www.certisign.com.br/certificado-digital. Acesso em: 24 out. 2018

McAfee LABS. **Relatório de segurança da informação**: dezembro de 2018. São Paulo, SP: McAfee, 2018. Disponível em: https://www.mcafee.com/enterprise/pt-br/assets/reports/rp-quarterly-threats-dec-2018.pdf Acesso em: 05 dez. 2018.

McAfee LABS. **Relatório de segurança da informação**: setembro de 2017. São Paulo: McAfee, 2017. Disponível em: https://www.mcafee.com/enterprise/pt-br/assets/reports/rp-quarterly-threats-sept-2017.pdf. Acesso em: 05 maios 2018.

LAUDON, Kenneth; LAUDON, Jane. **Sistemas de informação gerenciais.** 9. ed. São Paulo: Pearson, 2011.

MITNIK, Kelvin; SIMON, William. **A arte de enganar.** 4. ed. São Paulo: Pearson, 2003.

PEREIRA, Alex Sandro da Silva**. Bry Tecnologia**, 25 jun. 2018**.** Tipos de certificados digitais. Disponível em: http://www.bry.com.br/blog/tipos-de-certificados-digitais/. Acesso em: 21 out. 2018.

RAMOS, Anderson. **Guia oficial para formação gestores em segurança da informação.** São Paulo: Módulo Educação, 2007.

TOFLER, Alvin. **A terceira onda.** São Paulo: Record, 1985.