UNIVERSIDADE FEDERAL DO PARÁ
FACOMP – FACULDADE DE COMPUTAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

UMA ABORDAGEM SOBRE A SEGURANÇA DA INFORMAÇÃO NO MUNDO ATUAL

JOYCE DE ANDRADE MENDES

Castanhal-PA
2021

UNIVERSIDADE FEDERAL DO PARÁ
FACOMP – FACULDADE DE COMPUTAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

JOYCE DE ANDRADE MENDES

UMA ABORDAGEM SOBRE A SEGURANÇA DA INFORMAÇÃO NO MUNDO ATUAL

Trabalho de Conclusão de Curso submetido ao colegiado da Faculdade de Computação da Universidade Federal do Pará, como requisito parcial para a obtenção do grau de bacharel em Sistemas de Informação.

Orientador: Prof. Dr. Tássio Carvalho.

Castanhal-PA
2021

UNIVERSIDADE FEDERAL DO PARÁ
FACOMP – FACULDADE DE COMPUTAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

UMA ABORDAGEM SOBRE A SEGURANÇA DA INFORMAÇÃO NO MUNDO ATUAL

Trabalho de Conclusão de Curso apresentado ao Colegiado da Faculdade de Computação (FACOMP) da Universidade Federal do Pará do campus de Castanhal, como requisito parcial para a obtenção do Grau de bacharel em SISTEMAS DE INFORMAÇÃO.

_____
Prof. Dr. Tássio Carvalho
Orientador-UFPA/FACOMP

_____
Prof. Dr. Igor Ruiz Gomes
Membro da Banca – Filiação Membro 1

_____
Prof. Dr. José Jailton
Membro da Banca – Filiação Membro 2

_____
Prof. Dr. José Jailton
Diretor (a) da Faculdade de Computação - FACOMP

Castanhal-PA
2021

DEDICATÓRIA

Dedico este Trabalho de Conclusão de Curso a todos que me ajudaram nesta trajetória, principalmente à minha mãe Maria do Rosário e meu irmão Josimar de Andrade, que foram fundamentais para a minha formação.

AGRADECIMENTOS

Primeiramente eu gostaria de agradecer aos meus familiares que sempre me incentivaram e me ajudaram a continuar buscando meus objetivos, assim como os professores que me guiaram no meu caminho até aqui, em especial ao meu irmão, Josimar, que sempre foi o meu maior professor e, também, ao Professor Doutor Tássio Carvalho, por ser um excelente orientador.

"*A fé é a minha espada. A verdade é o meu escudo. O conhecimento é a minha armadura!*"
(*Estephen Stranger*)

Sumário

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

RESUMO

Na última década a tecnologia tem se tornado parte essencial do dia-a-dia das organizações e está cada vez mais presente na vida das pessoas, atualmente é um dos principais meios de comunicação. Desta forma, a quantidade de dados processados ou armazenados é imensurável e vão desde simples mensagens de texto até dados bancários e, para as organizações, seus dados representam um dos bens mais valiosos, sendo fundamental para a continuidade do negócio. Assim, a segurança da informação se torna fundamental não só no âmbito empresarial, mas também para a sociedade. Neste trabalho de conclusão de curso é abordado o tema de segurança da informação, seu conceito, finalidade, princípios, suas vulnerabilidades e o seu papel no mundo atual.

PALAVRAS-CHAVE: segurança, informação, dados, segurança da informação, segurança dos sistemas.

ABSTRACT

In the last decade, technology has become an essential part of the day-to-day life of organizations and is increasingly present in people's lives, it is currently one of the main means of communication. In this way, the amount of data processed or stored is immeasurable, ranging from simple text messages to bank details and, for organizations, their data represents one of the most valuable assets, being fundamental for business continuity. Thus, information security becomes essential, not only in the business sphere, but also for society. In this course conclusion work, the topic of information security, concept, purpose, principles, vulnerabilities and its role in today's world.

KEYWORDS: security, information, data, information security, systems security, cyber security.

1. Introdução

Segundo o Oxford Languages, entende-se como informação um conjunto de dados já analisados, integrados e interpretados que habilita alguém a tomar decisões seguras relativas a uma linha de ação e à conduta da manobra. Sendo a informação um bem cujo valor para uma organização não se pode estimar, é necessário a tomada de medidas que visem proteger esse bem de qualquer possível ameaça e é a Segurança da Informação (SI) que trabalha para assegurar a integridade desses dados sobre qualquer tipo de ameaça, utilizando de um conjunto de práticas, habilidades, recursos e mecanismos para proteger o sistema contra acesso indevido ou prevenir a perdas ou modificações de informações.

Segurança da informação trata de tudo aquilo que envolve a proteção de sistemas e dados de um determinado indivíduo ou organização. É papel da segurança da informação garantir que estes dados/sistemas estão realmente protegidos contra erros, furtos ou quaisquer incidentes aos quais as informações estão dispostas. O nível de segurança é estabelecido de acordo com o valor das informações e os potenciais prejuízos que podem ser causados por seu uso indevido.

1.1. Contextualização

A segurança da informação se caracteriza por um conjunto de ações que buscam manter dados seguros de modificações, perdas, cópias ou acessos indevidos. De acordo com o Tesauro Brasileiro de Ciência da Informação (Pinheiro e Ferrez, 2014) “a segurança da informação está relacionada à proteção e preservação da informação, e tem por finalidade evitar alterações, intencionais ou não, nos seus atributos de confidencialidade, integridade, disponibilidade e autenticidade. Não está restrita aos recursos computacionais e independe da forma como as informações/dados se apresentam: eletrônica, impressa etc”.

Pinheiro e Ferrez ainda apresentam a recuperação da informação como a questão central da ciência da informação, já o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) define segurança da informação como “um conjunto de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações”.

Atualmente, as principais normas que instruem sobre segurança da informação são da família ISO/IEC 27000. As mais conhecidas são as normas 27001 a 27005 que definem, na ordem, os critérios de implementação para um sistema de gestão de segurança da informação (SGSI), código de práticas para controles de segurança, guia de boas práticas, Monitorização,

medição, análise e avaliação das técnicas de segurança e por último, a norma 27005 trata da gestão de riscos, mas, ao todo, a família 27000 conta com mais de 40 normas, todas voltadas à segurança da informação, onde definem detalhadamente desde a criação da documentação relacionada à segurança, até a gerência de serviços como cloud computing, uso de aplicativos, gestão de incidentes, entre outros.

Além das normas ISO, no Brasil temos o Instituto Nacional de Tecnologia da Informação (ITI) que é responsável por cadastrar agentes e gerenciar entidades da ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira), que por sua vez, viabiliza a emissão de certificados digitais para a identificação virtual do cidadão, que é uma forma de autenticar informações digitais para que esta somente seja enviada ou recebida por pessoas autorizadas.

Algumas leis federais também dão a devida importância à segurança da informação, como a lei 13.709 de 14 de Agosto de 2018, que "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural", estabelecendo assim a Lei Geral de Proteção de Dados (LGPD).

Ainda em 2019 foi publicado a lei 13.853 que altera a lei citada anteriormente para dispor sobre a proteção de dados e criar a Autoridade Nacional de Proteção de Dados que tem a finalidade de fiscalizar e editar normas sobre o tratamento de dados.

1.2. Problemática da pesquisa

Com o crescente agregamento dos meios digitais no ambiente empresarial, cuidar da segurança dos sistemas tecnológicos de uma organização tornou- se uma das prioridades nesse meio. Com o aumento do uso de sistemas de informações digitais, houve também o aumento de interesses maliciosos. Não é qualquer pessoa que sabe lidar com problemas relacionados à tecnologia, por esse motivo, o número de ataques cibernéticos vem crescendo fortemente, cada vez que a tecnologia muda surge novos meios de tentar burlar a segurança dos dados.

Segundo estudo da Fortinet Threat Intelligence Insider Latin America, de janeiro a junho de 2020, apenas no Brasil, houveram 2,6 bilhões de tentativas de ataques, de um total de 15 bilhões em toda a América Latina e Caribe. Com o cenário de pandemia e a necessidade de trabalho remoto, denominado home office, "os criminosos encontram um número significativo de servidores RDP (remote desktop protocol) configurados incorretamente, o que reacende o interesse por ataque de força bruta, que são tentativas repetidas e sistemáticas de adivinhar uma

credencial enviando diferentes nomes de usuários e senhas para tentar acessar um sistema.", explica Alexandre Bonatti, diretor de engenharia da Fortinet Brasil.

1.3. Objetivo geral.

O objetivo geral deste trabalho é compreender a importância de uma política de segurança da informação no contexto global, as dificuldades encontradas na implementação de sistemas, bem como os principais riscos presentes nesta área, seu conceito básico e o papel que a segurança da informação representa no mundo atual.

1.3.1. Objetivos específicos

Este trabalho busca:

- especificar os princípios da segurança da informação, seus principais componentes e as ameaças às quais a informação está sujeita;
- Fazer uma análise das principais normas acerca da SI;
- Realizar uma pesquisa sobre a segurança da informação no cenário mundial atual.

1.4. Estrutura do trabalho

A estrutura deste trabalho está dividida entre uma pequena introdução sobre SI, resumos e análise de outros trabalhos referentes ao tema, um estudo da arte de segurança da informação onde é abordado os principais conceitos, ativos e ameaças, em seguida é feito uma análise das normas ISO/IEC 27001 e 27002, após isso é especificado os principais tipos de ataques a sistemas e os problemas que a segurança da informação enfrenta frequentemente, por último é apresentado o cenário de SI no mundo atual.

2. Estado da arte de Segurança da informação.

Neste parágrafo é feito o resumo e análise de diversos trabalhos sobre segurança da informação, com a intenção de agregar conhecimento e demonstrar as muitas possibilidades dentro do campo de SI.

2.1. Implantação de um sistema de gestão de segurança da informação: estudo de necessidades, criação e avaliação de um produto de informação, de Caroline Rogalsky.

Em seu trabalho, Rogalsky estuda as necessidades de segurança dentro de uma organização, pesquisando junto com profissionais locais as principais necessidades relativas à implementação de um sistema de gestão de segurança da informação (SGSI), registrando cada

etapa da pesquisa e utilizando dos dados obtidos para a criação um material de referência para a sua implementação, onde contém uma série de detalhes e especificações que auxiliam na conscientização da importância de um sistema de gestão para uma empresa, para que assim, haja uma melhor cooperação da organização durante os processos, uma vez que, quanto melhor informada, mais ativa é a participação da empresa no processo de implementação sendo avaliado pelos profissionais que participaram do levantamento das necessidades..

Para a criação do material de referência a autora realizou pesquisas em diversos trabalhos, artigos e livros sobre o tema, como a norma ISO 17799, o Orange Book, COBIT, BS 7799, entre outras, além de profundas entrevistas com profissionais de grandes empresas de Curitiba, observando suas expectativas e necessidades na área da segurança de dados. Inicialmente se planejava criar apenas um manual básico para a implementação de um SGSI, porém, após a coleta de dados nas entrevistas o trabalho evoluiu para um protótipo de guia que foi submetido à avaliação pelos mesmos profissionais que participaram anteriormente da entrevista.

Nas considerações finais a autora comenta sobre a escassez de materiais sobre o tema, seja eles feitos por brasileiros ou traduzidos de outras línguas, além disso, os entrevistados ressaltam algumas características negativas dos materiais já existentes como excesso de informação, falta de direcionamento e o fato de não serem feitos para leigos (com a presença de termos técnicos que dificultam a compreensão, desmotivando a leitura), o que resulta na falta de conhecimento sólido sobre o tema pelas empresas. A falta de material e de conhecimento possibilitou o cenário perfeito para a criação do material de referência nomeado GeSec.

2.2. “Um estudo de caso sobre a gestão da segurança da informação em uma instituição financeira”, de Raimundo Alan Matos Pessoa.

Neste trabalho o autor apresenta um estudo de caso sobre a gestão da segurança da informação na instituição financeira denominada ficticiamente “IFB”, onde o mesmo faz uma análise das práticas de controle relacionadas à segurança de informação implementadas na instituição com dois focos principais, política de segurança da informação e infraestrutura de Tecnologia da Informação, e se baseia nas normas ABNT NBR ISO/IEC 17799 - Tecnologia da informação - Técnicas de segurança - Código de prática para Gestão da Segurança da Informação e ABNT NBR ISO/IEC 27002 - Código de prática para a Gestão de Segurança da Informação para fazer uma avaliação de conformidade da gestão de segurança da organização em relação às normas e apresentar um comparativo com as práticas já aplicadas na instituição.

Primeiramente é abordado no trabalho os conceitos de informação, segurança da informação e seus princípios, gestão da segurança de informação e, também, uma pequena fala sobre o direito na informática. Após o autor descreve de forma resumida como funciona a política de segurança da informação, como os riscos devem ser analisados, avaliados e tratados, a infraestrutura adequada para assegurar a informação, gestão de segurança nos recursos humanos e físicos/ambientais, gerenciamento das operações, controle de acesso e desenvolvimento e manutenção de um sistema de informação, tudo isso baseado nas normas já citadas.

Por último é apresentado o estudo de caso, realizado com o intuito de avaliar a situação atual de segurança da informação na instituição. Os métodos e técnicas utilizados na pesquisa foram observação direta, onde foi observado o dia-a-dia de trabalho na agência e entrevistas com os responsáveis do setor de tecnologia de informação-TI com o objetivo de coletar dados acerca da segurança da informação na empresa, também foram feitas entrevistas com o gerente executivo de TI e o gerente executivo da agência com o foco na política e na infraestrutura de SI. Todos os dados da empresa referentes à gestão, estrutura organizacional e segurança de informação são apresentados no trabalho. Após a coleta de dados foi feito um questionário verificador de conformidade de acordo com as normas de referência onde, de acordo com as respostas, se constatou que a empresa se baseia na norma ABNT NBR ISO/IEC 27002.

2.3. “A Segurança da Informação nas Redes Sociais”, de Leandro Farias dos Santos Abreu.

Este trabalho aborda a segurança da informação com foco nas redes sociais. De início o autor explica o conceito de segurança da informação e seus princípios básicos: confidencialidade, integridade e disponibilidade. Depois aborda os mecanismos de segurança necessários para dar suporte aos princípios básicos como controles físicos, onde o acesso à informação é limitado por infraestrutura e controles lógicos, que impedem o acesso por meio eletrônico, como criptografias, assinatura digital e autenticação.

Após a explicação básica sobre SI o autor entra no meio das redes sociais falando sobre as senhas, que é um dos principais mecanismos para garantir o controle de acesso aos dados. Senhas mal elaboradas ou de fácil dedução podem dar acesso à diversas informações confidenciais, considerando que atualmente as redes sociais vão além do entretenimento e acabam se tornando uma grande ferramenta de negócios e socialização, podendo conter, assim, informações críticas sobre alguém, como contas de banco ou outras senhas de acesso.

Depois das senhas é abordado os riscos no uso da internet como execução de programas e acesso a sites não confiáveis, transações comerciais sem nenhum mecanismo de segurança, leitura de emails com vírus, vulnerabilidades de software e trocas de mensagens onde o atacante pode usar de engenharia social para induzir a vítima a dar informações confidenciais como número de cartão de crédito.

Após os riscos é apresentado os mecanismos de segurança que podem ser utilizados no uso da internet, como antivírus, firewalls, proxies e backups, explicando o conceito de cada um. Entrando no tema do artigo o autor faz uma comparação entre mídias sociais e redes sociais exemplificando os principais sites que fazem parte desse meio e abordando a questão da privacidade e segurança e dando exemplos de ataques e incidentes logo após falando sobre o papel das redes sociais nos crimes virtuais.

2.4. "O enfoque social da segurança da informação", de João Luiz Marciano e Mamede Lima-Marques.

Este artigo faz uma interessante abordagem de como o meio social pode ser afetado pela falta da segurança de informação, prejudicando a segurança das pessoas, suas informações e quaisquer interações feitas no meio digital. Vem, assim, propor a "*integração de disciplinas oriundas do âmbito das ciências sociais para a construção de um arcabouço destinado à elaboração, implementação e acompanhamento de políticas de segurança abrangentes, que contemplem com o adequado equilíbrio os aspectos humanos e técnicos da segurança da informação, em contraposição aos modelos atuais, notadamente voltados às questões tecnológicas*".

O artigo, primeiramente, realiza uma análise do comportamento do usuário de sistemas de informações com foco nas suas interações sociais, buscando referências nas ciências sociais como sociologia, psicologia e antropologia para a realização da pesquisa, utilizando uma abordagem baseada na interação simbólica para analisar o comportamento social.

Por último, os autores exploram a abrangência da segurança de informação citando as normas padrões (ABNT NBR ISO/IEC 17799 e 27002), demonstrando um foco maior voltado para a tecnologia dos sistemas. Por isso os autores formulam o conceito de segurança da informação e, para finalizar, fazem a sugestão de alguns princípios éticos e legais que venham a governá-la

2.5. “Estudo sobre a quebra de confidencialidade da informação e mecanismos de segurança”, de Tatieli Zanella.

Este trabalho faz uma avaliação da importância da segurança da informação, mesmo para empresas pequenas, o objetivo geral foi sistematizar os principais tipos de ataque, mecanismos de segurança e ferramentas relacionadas com a quebra de confidencialidade de informações que podem ocorrer dentro de uma organização e os resultados do estudo foram aplicados em uma empresa de pequeno porte.

Primeiramente a autora define os conceitos de segurança de informação, bem como seus princípios básicos e faz uma análise acerca das principais ameaças existentes e mecanismos de segurança da informação como protocolos de rede, softwares que auxiliam na segurança ou monitoram o tráfego da rede e mecanismos gerenciais, físicos, de codificação, entre outros, que são parte fundamental para garantir a integridade das informações.

Na proposta de solução a autora selecionou uma empresa de pequeno porte, realizou a análise do cenário corporativo aplicando um questionário quanto à SI da organização, analisando os objetivos protecionistas e os aspectos econômicos da organização, o levantamento de possíveis ameaças que podem ocorrer durante o ciclo de vida da informação e a definição e testes de ferramentas que podem auxiliar na prevenção de ataques e correção de riscos através de uma estratégia operacional. Após a aplicação dos mecanismos de segurança foi feito outro questionário para avaliar os resultados.

Na conclusão do trabalho é apresentado o estudo de caso onde é mostrado resumidamente o cenário atual da empresa, como o organograma que conta com o gerente, setor de suporte, financeiro, comercial e desenvolvimento, a infraestrutura tecnológica da empresa, como a quantidade de computadores, softwares que auxiliam na gestão e segurança e situação do servidor local. Após toda a análise do cenário empresarial, pôde-se definir os principais riscos aos quais a empresa estava submetida.

Devido à baixa complexidade dos processos, a análise de gestão de riscos foi aplicada em todos os processos da empresa, desde compras e vendas até atendimento aos clientes e à área de TI. Após toda a coleta de dados e análises a autora apresentou à empresa o seu trabalho, mostrando os principais riscos identificados e apresentando propostas de soluções e melhorias para a organização de forma que todos os colaboradores conseguiram identificar a importância da segurança da informação no âmbito corporativo.

2.6. “O impacto da engenharia social na segurança da informação:uma abordagem orientada à gestão corporativa”, de João Paulo Aramuri e Luiz Cláudio Maia.

A maioria dos sistemas digitais possuem bons sistemas de segurança, tornando-os difíceis de invadir através de um ataque externo. Por isso, muitos criminosos optam por engenharia social para realizar ataques, que “são facilitados” por pessoas de dentro das organizações. Aramuri e Maia apresentam uma abordagem sobre como a engenharia social tem influenciado na segurança da informação das organizações, identificando as principais vulnerabilidades existentes nesse meio, além de expor a problemática relacionada à forma como a engenharia social é utilizada para extraviar informações sigilosas da empresa.

Após fazer uma pequena introdução sobre o principal problema da temática, citando diversas referências, dentre elas Eiras (2004), que diz: "A engenharia social evita a criptografia, segurança de computador, segurança de rede e tudo o mais que for tecnológico. Ela vai diretamente para o elo mais fraco de qualquer sistema de segurança: O ser humano”. Essa técnica se aproveita de pessoas com pouco ou nenhum treinamento acerca dos riscos no âmbito digital, para realizar invasões de sistemas, roubos de dados, alterações de informações importantes, dentre outros atos prejudiciais à empresa.

Os autores apontam alguns traços comportamentais que tornam o ser humano suscetível a esse tipo de ataque, são estes:

a) Persuasão - o funcionário pode ser induzido a dar informações através de manipulação para conseguir respostas específicas que, muitas vezes, parecem até inofensivas, mas que podem ser utilizadas por criminosos de diversas maneiras;
b) Vontade de ser útil - o ser humano, comumente, procura agir com cortesia, e é em uma dessas buscas de ajudar o próximo que pode acabar sendo vítima de engenharia social;
c) Busca por novas amizades - quando elogiado, o ser humano se agrada e se sente bem, o que o torna mais aberto a conversas que podem conter informações importantes;
d) Propagação de responsabilidade - situação onde o funcionário considera que a responsabilidade sobre certa atividade não é somente sua, podendo deixar vulnerável alguma parte do sistema.

Sendo assim, se considera a engenharia social uma falha no sistema tão grave quanto qualquer outro ataque. Assim como uma organização necessita de antivírus e firewalls, também é preciso investimento para instruir os funcionários sobre ações que podem prejudicar a empresa. “*A segurança da informação está mais relacionada com os processos e as pessoas do que com a própria tecnologia. Dessa forma, não há vantagem em investir pesado em tecnologia e deixar de lado o fator humano*”.

2.7. Análise dos trabalhos.

Todos os trabalhos relatados aqui têm foco em diferentes áreas da Segurança da informação, desde processos de implementação e gestão até o uso de engenharia social para ataques corporativos. Os dois primeiros trabalhos estão relacionados com as necessidades dentro de uma organização, quais normas deve-se seguir para implementar um SI, o que deve-se levar em consideração, quais medidas devem ser adotadas, entre outras especificações. Rogalsky faz uma pesquisa aprofundada em diversas organizações, falando diretamente com os responsáveis de segurança sobre suas principais necessidades. Já Pessoa estuda como uma instituição adapta as normas vigentes dentro da organização, seu estudo alcança toda a gestão de segurança da informação, desde políticas, até a infraestrutura envolvida.

Diferente dos trabalhos anteriores, Leandro Farias aborda a SI nas redes sociais, dando ênfase nos riscos aos quais os usuários estão expostos e como o comportamento do próprio influencia na sua segurança na internet. Já Marciano e Marques abordam como a falta de segurança afeta o meio social e seus indivíduos, se utilizando de conceitos da sociologia e psicologia para fazer referências às interações entre usuário e mídias sociais.

Zanella apresenta um pequeno estudo sobre como a segurança da informação também é importante nas pequenas empresas, em seu trabalho a autora avalia uma organização de pequeno porte e implementa princípios básicos de SI, em sua monografia Zanella mostra que, mesmo em negócios pequenos a informação deve ser tratada como um ativo importante. Já Aramuri e Maia focam seu trabalho em um tipo específico de ataques às corporações, a engenharia social, mostrando as principais vulnerabilidades as quais as empresas estão expostas e os principais fatores que influenciam na ocorrência destes ataques.

Todos os trabalhos apresentados nesta seção nos apresentam diferentes âmbitos da segurança da informação, evidenciando sua vastidão e importância nas organizações.

3. Estudo acerca da Segurança da Informação

A Segurança da Informação engloba diversos elementos, que são fundamentais para a sua existência, como a informação propriamente dita e os vários ativos que fazem parte da vida da informação. A seguir é analisado os componentes que sustentam a SI, que servem como base para tudo que a SI trata.

3.1. Informação

Original do latim, *informare,* significa modelar, dar forma. Entende-se como informação qualquer conjunto de dados organizados e relacionados a algo específico que tenha valor para alguém, seja pessoa ou organização. Tem como objetivo contribuir para a construção

ou aprofundação de conhecimento ou eliminação de incertezas acerca de determinado assunto ou esclarecer o funcionamento de processos ou objetos. A informação é capaz de dar origem à formação do pensamento humano, através da sua análise é possível tomar decisões e resolver problemas com base no uso racional do conhecimento adquirido, portanto, quanto mais precisa a informação, melhor.

No âmbito organizacional a informação é tratada como item de extrema importância, sendo um dos itens principais para a formação e implementação de processos ou melhorias e servindo como base para qualquer atividade realizada dentro de um sistema.

3.2. Segurança da Informação

Sendo a informação algo tão importante para a sociedade, é extremamente necessário criar mecanismos para a manipulação segura desses dados. Primeiramente a informação não pode se perder, portanto é preciso garantir a sua integridade, dependendo do contexto, o acesso à informação também precisa ser restrito para garantir a sua confidencialidade e descrição. Pela sua importância é necessário garantir que a informação está segura, para isso existe a segurança da informação, que dita práticas, recursos e mecanismos necessários para garantir que a informação esteja segura.

Segurança da informação se trata de tudo aquilo que envolve a proteção de dados, seu papel é assegurar que a informação não sofrerá alteração, perda, acesso indevido, roubo ou qualquer outro infortúnio. O gerenciamento de segurança deve ser adotado de acordo com a relevância que a informação possui.

Figura 1: Representação da tríade CIA

Fonte:ESET Portugal

Os princípios básicos da segurança da informação, representados pela tríade CIA - Confidencialidade, Integridade e Disponibilidade (*Confidentiality, Integrity and Availability*), mostrados na figura 1, apresentam os principais aspectos que devem ser levados em consideração quando se pensa em segurança e servem como referência para análise, planejamento e implementação de técnicas de segurança da informação em qualquer sistema.

- Confidencialidade

O valor da informação está de acordo com a sua importância, quanto mais precisa e detalhada, mais valiosa se torna. Para uma empresa a informação pode ser a chave de todo o sucesso ou o motivo do seu fracasso. A confidencialidade significa que os dados estejam seguros de acesso indevido, que apenas serão acessados por pessoas autorizadas pois, normalmente, são informações críticas para uma organização, que contém dados sobre seus produtos ou informações dos processos internos da organização.

- Integridade

Assim como a confidencialidade, manter a integridade das informações é extremamente importante, partindo do pressuposto que os setores de uma instituição estão todos ligados e, sendo a informação a base para os processos de um sistema, uma simples alteração indevida pode bagunçar toda a organização e resultar na perda de recursos e prejuízos que são difíceis de se imaginar. Manter a integridade das informações é garantir que esses dados não serão adulterados, corrompidos, destruídos ou perdidos e, juntamente com a Confidencialidade, garantir que não terão acessos indevidos.

- Disponibilidade

Enquanto a Confidencialidade e a Integridade buscam garantir uma proteção à informação contra o acesso não autorizado, o conceito de Disponibilidade é garantir que a informação está acessível à quem lhe interessa e, por isso, também se torna algo de extrema importância em qualquer sistema. A impossibilidade de consultar dados pode significar um atraso nos processos, que por sua vez, dependendo da organização, pode ter resultados extremamente ruins, como a perda de clientes ou recursos. “Tempo é dinheiro” é a frase perfeita para esta situação, por isso a importância de garantir que a informação esteja disponível para ser consultada a qualquer momento.

Além da tríade, recentemente, também surgiram novos atributos de segurança da informação, como a autenticidade e a privacidade, que buscam se certificar que as informações

são verdadeiras e, no caso de dados compartilhados entre um grupo específico de usuários, estarão seguras de acessos por pessoas que não fazem parte do grupo de acesso.

3.3. Ativos da informação

A segurança da informação dita, de forma geral, como a informação deve ser tratada para garantir sua seguridade e quais são os principais aspectos que devem ser levados em consideração na hora de implementar um sistema de gestão de segurança e refere-se à constante proteção dos dados em si, dos sistemas e da infraestrutura e dos serviços que a suporta.

Os ativos da informação se referem a todos os componentes que fazem parte do universo da informação, é neles que são aplicados quaisquer planos ou normas de segurança, são os principais atuantes na segurança da informação. Os elementos que compõem os ativos da informação são: a própria informação, os equipamentos (hardware) e sistemas (software) e as pessoas que fazem uso desse conjunto. É importante garantir a adequada segurança dos ativos, pois são eles que dão sustentabilidade para os negócios, a demonstração de qualquer problema já coloca a toda a organização em risco.

Os ativos são descritos da seguinte maneira:

- Informação

  As informações da organização podem ser guardadas em ambiente lógico, como tabelas e documentos digitais, ou ambiente físico onde todos os dados como relatórios, planilhas, fichas de funcionários, entre outros, são impressos e armazenados em um local considerado seguro.

- Hardware

  Envolve toda a infraestrutura tecnológica de uma organização pela qual a informação é processada, armazenada e utilizada, como computadores, servidores, mídias de armazenamento externo, entre outros.

- Software

  É a parte lógica que contribui para a segurança da informação, desde sistemas operacionais até antivírus utilizados pelos hardwares, permitindo o processamento, acesso e leitura dos dados.

- Usuário

  São todas as pessoas envolvidas nos processos da organização e que podem ter acesso à alguma informação.

Independente de se utilizar meios tecnológicos ou não para armazenar e gerenciar as informações, é necessário sempre garantir que o meio ao qual a informação está inserida é seguro tanto de ataques, quanto de desastres naturais. Para implementar um projeto de segurança da informação em uma organização é preciso estabelecer as diretrizes e mecanismos de segurança, definir as políticas de processos e procedimentos, as ferramentas tecnológicas de proteção e garantir o comprometimento das pessoas envolvidas no processo.

3.4. Principais ameaças

Devido à constante evolução da tecnologia, se faz necessário a, também constante atualização dos meios de segurança, pois deve-se supor que os sistemas estão sob constante ameaça. Qualquer que seja o meio, um sistema sofre ameaças de todos os lados, desde ataques tecnológicos, indícios de acidentes ou ataques à infraestrutura onde a informação está guardada, qualquer coisa que signifique a perda, destruição ou modificação indevida da informação é sinal de ameaça e deve estar inserida em um sistemas de gestão de riscos onde serão tratados e prevenidos de acordo com seu grau de importância.

Existem três principais componentes que fazem parte do cenário de ameaças iminentes, hardware, software e pessoas e cada um deles é abordado a seguir:

- Hardware

  A infraestrutura onde a informação está sendo guardada normalmente é considerada um sistema seguro, principalmente se tratando de uma estrutura tecnológica. Porém, ultimamente já se apresentam alguns sinais preocupantes da degradação desse sistema considerado tão seguro. Um exemplo disso é a descoberta recente de pesquisadores do Project Zero da Google que encontraram uma vulnerabilidade que afeta a memória RAM DDR3, a falha atinge a troca de informação entre a memória e a placa mãe fazendo com que uma parte específica da memória seja acessada centenas de milhares de vezes levando a modificações em pequenas frações de informações e, até alterações de dados do sistema operacional. A falha poderia ser usada para manipular o computador e abre a possibilidade de acessar e alterar o sistema. Até agora o problema

foi identificado apenas nos modelos de memória RAM DDR3, porém, por ser um problema de hardware a preocupação está na indefinição de uma solução e a possibilidade de falhas semelhantes afetarem outras partes físicas do sistema. Apesar de preocupante, essa ameaça ainda é muito recente e pouco estudada, ainda não se sabe o padrão de atuação nem todas as possibilidades que a falha dá a invasores.

As ameaças ao hardware não estão definidas apenas devido a falhas nos seus sistemas, mas também ao ambiente onde a estrutura está inserida. Como qualquer outro ambiente físico, também está sujeito a ataques, violações ou acidentes.

- Software

As principais ameaças ao software estão relacionadas a falhas que oferecem brechas para possíveis ataques, é importante ter em mente os objetivos de um invasor e um bom conhecimento da arquitetura do software e suas vulnerabilidades para que se possa identificar as possíveis ameaças e criar meios de prevenção e reparo,

4. Análise das normas ABNT NBR ISO/IEC 27001 e 27002.

Garantir a segurança das informações é crucial para qualquer empresa, porém, definir ações para assegurar esses dados pode ser um desafio, por isso, foram criadas as normas da família 27000, a fim de proporcionar às organizações de qualquer tamanho, parâmetros que auxiliam na Segurança da Informação. As normas NBR ISO/IEC 27000 até 27007 descrevem, justamente, modelos a serem seguidos na implementação de sistemas de gestão de segurança da informação, desde os requisitos necessários, às práticas, implementação, gestão e continuação.

A implementação das normas da família 27000 (que conta com mais de quarenta documentos), garante a continuidade de negócio através da avaliação, tratamento e gestão de riscos com o intuito de diminuir o impacto de incidentes que venham a acontecer. Cada uma das normas é voltada para um aspecto do SGSI e juntas se complementam. Abaixo é apresentado algumas das principais normas da família 27000 e após, resumos das normas 27001 e 27002.

- 27000 - Visão geral e vocabulário de SI;
- 27001 - requisitos de um SGSI;
- 27002 - código de prática de um SGSI;
- 27003 e 27004 - gestão de SI e guia de implementação de SGSI;

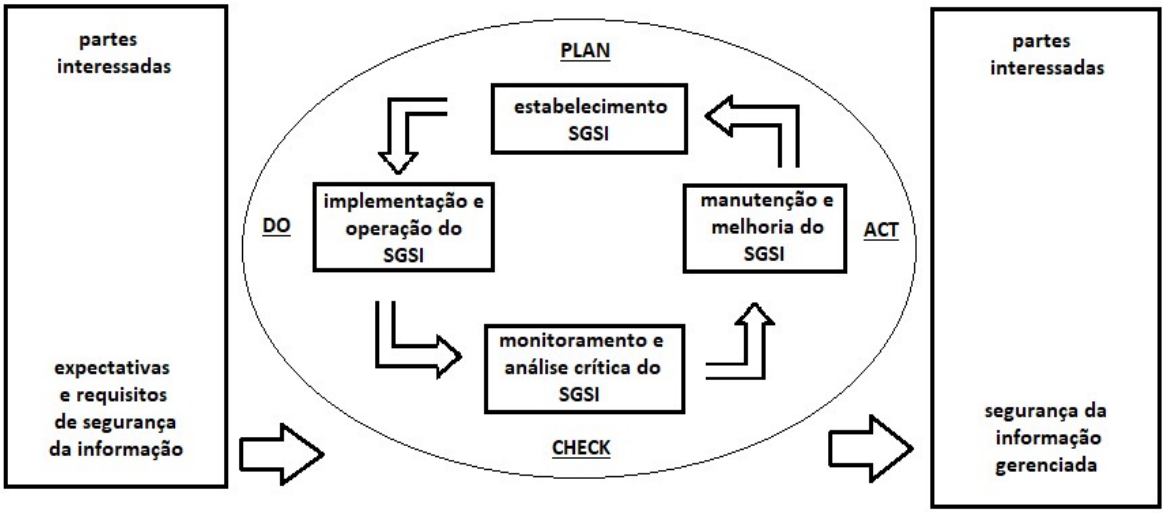
- 27005 - diretrizes de processos de gestão de riscos de um SGSI;
- 27006 e 27007 - requisitos e diretrizes para auditoria de SGSI.

4.1. Norma ABNT NBR ISO/IEC 27001:2013

Sendo a primeira norma da família 27000, a ISO 27001 é uma norma internacional emitida pela Organização Internacional de Normalização e "provê um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)" [ABNT NBR ISO/IEC 27001, ABNT 2006]. A norma, que é uma evolução da antiga BS7799:2 do Reino Unido, certifica as organizações em termos de gestão de segurança da informação e pode ser adaptada para todos os tamanhos de negócios, se adequando às necessidades e realidade da organização, seus objetivos e sua estrutura.

A norma utiliza o modelo conhecido como *Plan-Do-Check-Act* (PDCA), que é aplicado para estruturar todos os processos do SGSI. Na imagem 2 está representado as fases do ciclo, ilustrando como o SGSI considera as entradas dos requisitos de segurança juntamente com a expectativa das partes interessadas, e como todo o processo de segurança resulta no atendimento destes requisitos.

Figura 2. Modelo PDCA aplicado aos processos do SGSI



Fonte: Norma ISO 27001

- Plan (planejar) (estabelecer o SGSI)

  "Estabelecer a política, objetivos, processos e procedimentos do SGSI relevantes para a gestão de riscos e a melhoria da segurança da informação para

produzir resultados de acordo com as políticas e objetivos globais de uma organização", [ABNT NBR ISO/IEC 27001, ABNT 2006]. Ou seja, antes de começar a implementar qualquer coisa, é preciso avaliar a realidade da organização, quais suas necessidades, objetivos e prioridades e, a partir disso, traçar um plano de ações que se encaixe no contexto da organização.

- Do (fazer) (implementar e operar o SGSI)
  "Implementar e operar a política, controles, processos e procedimentos do SGSI", [ABNT NBR ISO/IEC 27001, ABNT 2006]. Uma vez traçado o plano de ação para estabelecer o SGSI é hora de iniciar a implementação.
- Check (checar) (monitorar e analisar criticamente o SGSI)
  "Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção", [ABNT NBR ISO/IEC 27001, ABNT 2006]. Após a fase de implementação vem a análise, onde o sistema será avaliado de acordo com os requisitos que foram estabelecidos previamente, para ter certeza que o plano de ação está cumprindo com o esperado e planejado na fase *Plan*, então é preciso monitorar o sistema e medir se os objetivos foram atingidos.
- Act (agir) (manter e melhorar o SGSI)
  "Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI", [ABNT NBR ISO/IEC 27001, ABNT 2006]. A gestão de uma organização nunca fica estagnada, sempre haverá mudanças a se fazer, pois a evolução é contínua. Portanto, após a checagem do sistema, vem a fase de correções, mudanças, alterações que devem ser feitas para corrigir o sistema, caso não esteja atingindo o objetivo da organização, ou a implementação de melhorias para tornar os processos mais eficazes.

Além de utilizar o modelo *Plan-Do-Check-Act*, a norma 27001 está alinhada às normas ISO 9001, de sistemas de gestão de qualidade, e 14001, de gestão ambiental, para a implementação de um sistema adequado a outras normas de gestão que estão relacionada com a 27001. A tabela 1 mostra a relação correspondente entre as normas.

Tabela 1 — Correspondência entre a ABNT NBR ISO 9001:2000, 14001:2004 e 27001.

Esta norma	**ABNT NBR ISO 9001:2000**	**ABNT NBR ISO 14001:2004**

0 Introdução 0.1 Geral 0.2 Abordagem de processo 0.3 Compatibilidade com outros sistemas de gestão	**0 Introdução** 0.1 Geral 0.2 Estratégia do processo 0.3 Relação com ABNT NBR ISO 9004 0.4 Compatibilidade com outros sistemas de gestão	**0 Introdução**
1 Objetivo 1.1 Geral 1.2 Aplicação	**1 Objetivo** 1.1 Generalidades 1.2 Aplicação	**1 Objetivo**
2 Referências normativas	**2 Referências normativas**	**2 Referências normativas**
3 Termos e definições	**3 Termos e definições**	**3 Termos e definições**
4 Sistema de gestão de segurança da informação 4.1 Requisitos gerais 4.2 Estabelecendo e gerenciando o SGSI 4.2.1 Estabelecer o SGSI 4.2.2 Implementar e operar o SGSI 4.2.3 Monitorar e analisar criticamente o SGSI	**4 Sistema de gestão da qualidade** 4.1 Requisitos gerais 8.2.3 Medição e monitoramento de processos 8.2.4 Medição e monitoramento de produtos	**4 Requisitos do SGA** 4.1 Requisitos gerais 4.4 Implementação e operação 4.5.1 Monitoramento e medição
4.2.4 Manter e melhorar o SGSI		
4.3 Requisitos de documentação 4.3.1 Geral 4.3.2 Controle de documentos	4.3 Requisitos de documentação 4.3.1 Geral 4.3.2 Manual da qualidade 4.3.3 Controle de documentos	4.4.5 Controle de documentos 4.5.4 Controle de registros

4.3.3 Controle de registros	4.3.4 Controle de registros	
5 Responsabilidades da direção 5.1 Comprometimento da direção	**5 Responsabilidades de gestão** 5.1 Comprometimento da direção 5.2 Foco no cliente 5.3 Política da qualidade 5.4 Planejamento 5.5 Responsabilidade, autoridade e comunicação	4.2 Política ambiental 4.3 Planejamento
5.2 Gestão de recursos 5.2.1 Provisão de recursos 5.2.2 Treinamento, conscientização e competência	**6 Gestão de recursos** 6.1 Provisão de recursos 6.2 Recursos humanos 6.2.2 Competência, conscientização e treinamento 6.3 Infraestrutura 6.4 Ambiente de trabalho	4.2.2 Competência, treinamento e conscientização
6 Auditorias internas do SGSI	8.2.2 Auditorias internas	4.5.5 Auditorias internas
7 Análise crítica do SGSI pela direção 7.1 Geral 7.2 Entradas para a análise crítica 7.3 Saídas da análise crítica	**5.6 Análise crítica pela direção** 5.6.1 Generalidades 5.6.2 Entradas para a análise crítica 5.6.3 Saídas para análise crítica	**4.6 Análise pela administração**
8 Melhoria do SGSI 8.1 Melhoria contínua 8.2 Ações corretivas	**8.5 Melhorias** 8.5.1 Melhoria contínua 8.5.3 Ações corretivas	4.5.3 Não-conformidades, ação corretiva e ação preventiva

8.3 Ações preventivas	8.5.3 Ações preventivas	
Anexo A - Objetivos de controle e controles; Anexo B - Princípios da OECD e esta Norma; Anexo C-Correspondência entre a ABNT NBR ISO 9001:2000, a ABNT NBR ISO 14001:2004 e esta Norma	**Anexo A - Correspondência entre a ABNT NBR ISO 9001:2000 e a ABNT NBR ISO 14001:2004.**	**Anexo A - Guia para o uso desta Norma; Anexo B - Correspondência entre ABNT NBR ISO 14001:2004 e ABNT NBR ISO 9001:2000**

Fonte: ABNT NBR ISO/IEC 27001:2006, anexo C.

A norma está dividida em nove sessões, sendo estas, introdução (0), objetivo (1), referência normativa (2), termos e definições (3), sistema de gestão de SI (4), responsabilidades da direção (5), auditorias internas de SGSI (6), análise crítica do SGSI pela direção (7) e melhoria do SGSI (8). Das seções 0 a 3 a norma traz um nivelamento teórico, explicando ao que a norma se propõe. Na introdução temos uma pequena apresentação da norma e do modelo PDCA, conceituando cada fase do modelo e apresentando as normas compatíveis com esta.

Na sessão de objetivos é descrita a função da norma dentro da organização, que é "especificar os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização'. Ela especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes", [ABNT NBR ISO/IEC 27001, ABNT 2006], ou seja, a norma está focada nos requisitos que a empresa deve atender para conseguir implementá-la, quais requisitos podem ser adaptados à organização, quais são aceitáveis de exclusão e quais não são.

Na referência normativa é referenciado à norma ABNT NBR ISO/IEC 17799:2005, Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação, norma esta considerada indispensável para a aplicação da 27001. Em termos e definições é apresentado um pequeno glossário da norma com as definições dos termos usados ao longo do documento.

Nas seções de 4 a 8 a norma apresenta todos os requisitos para a organização estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um

SGSI. Começando pela seção 4 que especifica todas as fases do SGSI, desde o estabelecimento do sistema, sua implementação e operação, o monitoramento e a análise crítica, até o seu melhoramento, incluindo também os requisitos para a documentação do sistema. Já na seção de responsabilidades da direção, é especificado o comprometimento que a direção deve ter frente ao sistema, estabelecendo políticas, estabelecendo o plano, objetivo, papéis e responsabilidades dentro da implementação do sistema, a provisão e gestão de recursos e a comunicação à organização da importância de atender os critérios estabelecidos.

A seção 6 se refere a condução de auditorias internas do SGSI em intervalos planejados para verificar se os e objetivos e processos estão se encaminhando adequadamente dentro da norma e da legislação, se estão atendendo os requisitos de segurança da informação e se estão sendo implementados e executados de forma eficaz, conforme o esperado. Na seção 7 especifica as entradas para uma análise crítica que deve ser feita pela direção em intervalos planejados, a fim de manter o bom funcionamento e eficácia do SGSI, deve incluir a avaliação de oportunidades para melhoria e a necessidade de mudanças do SGSI, onde tudo deve ser documentado e os registros devem ser mantidos.

A última seção da norma, sobre melhoria contínua, traz especificações sobre ações corretivas que devem ser aplicadas e documentadas para garantir continuamente a melhora da eficácia do sistema na organização, assim como ações de prevenção para identificar e eliminar causas de não-conformidade com os requisitos do SGSI que devem estar apropriadas aos impactos dos potenciais problemas.

4.2. Norma ABNT NBR ISO/IEC 27002:2013

Esta norma, sendo a segunda da família 27000, apresenta um código de prática para a implementação, gestão e continuidade de um sistema de gestão de segurança da informação. Enquanto a norma 27001 apresenta um plano de projetos que guia a organização dentro do SGSI, a norma 27002 traz os controles necessários para isso de forma mais definida, detalhando melhor cada processo e cada etapa, desde a organização da segurança da informação até a continuidade de negócio, servindo, assim, como um guia completo para organizações que desejam implementar ou melhorar seu sistema de segurança. A norma “fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização”, [ABNT NBR ISO/IEC 27002:2013].

Dividida em 18 seções, mais a introdução. A norma apresenta em cada seção, itens que oferecem indicações sobre o controle da segurança da informação. Nas seções de 1 a 4 temos a apresentação do documento da norma, apresentando seu escopo, referência normativa, termos e definições, onde é referenciada à norma ISO/IEC 27000, e a estrutura da norma que conta com 14 seções de controles de segurança da informação de um total de 35 objetivos de controle e 114 controles. As definições da norma são apresentadas a partir da seção 5:

4.2.1. Seção 5, sobre política de SI.

É apresentado uma orientação da direção e apoio para a segurança da informação de acordo com os requisitos do negócio e as leis e regulamentações relevantes e indica a criação de um documento relativo à segurança da informação da empresa onde deve ser definido um conjunto de políticas de segurança, as diretrizes de implementação, uma estrutura para estabelecer os objetivos e as formas de controle, o comprometimento da direção com a política, atribuição de responsabilidades e processos para o tratamento dos desvios e exceções.

"Ao estabelecer uma política para a segurança da informação, a administração provê as diretivas e o apoio para a organização. Essa política deve ser escrita em conformidade com os requisitos do negócio, bem como as leis e os regulamentos relevantes", [Hintzbergen, Smulders e Baars, 2018]. Além de estar de acordo com a legalidade, a política de segurança deve ser aprovada pela administração e apresentada aos funcionários de todos os níveis, assim como fornecedores e clientes, pode ser anunciada de forma resumida, deixando claro seus pontos principais, deixando a versão completa a disposição dos interessados.

4.2.2. Seção 6, sobre organização da segurança da informação.

O objetivo é "estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização", [ABNT NBR ISO/IEC 27002:2013] . A definição das responsabilidades e papéis da segurança da informação é o foco desta seção, especificando quais papéis devem ser atribuídos e quais suas responsabilidades, como a responsabilidade pela proteção de ativos e cumprimentos de processos e pelas atividades de gerenciamento de riscos.

Os responsáveis pela segurança da informação podem delegar atividades a outros indivíduos, porém, ainda é de sua responsabilidade a correta execução das tarefas que foram delegadas. As funções que interferem ou entram em conflitos com outras áreas devem ser segregadas, para reduzir os riscos de modificações não autorizadas ou o uso indevido de ativos.

“Segregação de funções é um método para reduzir o risco de mau uso, acidental ou deliberado, dos ativos de uma organização”, [ABNT NBR ISO/IEC 27002:2013].

O contato com as autoridades também é enfatizado nesta seção, é necessário saber quais autoridades devem ser contatadas em caso de incidentes e como o ocorrido deve ser relatado sem comprometer a segurança das informações. Assim como o contato com autoridades, manter contato com grupos especiais também é importante, grupos especiais de profissionais ou outros fóruns de segurança da informação que podem vir a agir em determinadas situações, esse tipo de contato serve para ampliar conhecimento sobre as melhores práticas, se manter atualizado sobre questões de segurança, recebe previamente alertas, aconselhamentos e correções relativos à ataques e vulnerabilidades. acesso à consultoria especializada e troca de informações sobre novas tecnologias, produtos, ameaças e vulnerabilidades.

4.2.3. Seção 7, sobre gestão de recursos humanos.

Sendo a participação humana de extrema importância para todos os processos do sistema de gestão de segurança da informação, também é de extrema importância reservar uma atenção especial para essa gestão e a seção 7 trata exatamente disso, “convém que verificações do histórico sejam realizadas para todos os candidatos a emprego, de acordo com a ética, regulamentações e leis relevantes, e seja proporcional aos requisitos do negócio, aos riscos percebidos e à classificação das informações a serem acessadas”, [ABNT NBR ISO/IEC 27002:2013].

Para tanto, é necessário a adoção de medidas preventivas no ato da seleção de candidatos, como referências profissionais e pessoais, verificação das informações contidas no currículo do candidato, confirmação das qualificações, verificações de crédito ou antecendentes criminais, além de ter a competência necessária e ser confiável para desempenhar o papel designado, principalmente se for um papel crítico na organização. Após a contratação, ainda é preciso manter verificações constantes de controle.

Para os termos e condições de contratação é necessário que seja especificado em contrato as obrigações dos funcionários, refletindo as políticas de segurança da empresa esclarecendo e declarando: a necessidade de um termo de confidencialidade para todos que tenham acesso à informações sensíveis, às responsabilidades legais e direito de todas as partes envolvidas, as responsabilidades pela classificação das informações e o gerenciamento de ativos, as responsabilidades das partes envolvidas no tratamento de informações recebidas de outras companhias ou partes interessadas e, por último, as ações que devem ser tomadas em

caso de desrespeito aos requisitos de segurança. Todos os papéis e responsabilidades devem ser comunicados antes da contratação efetiva e o contratado deve estar de acordo com as condições.

É responsabilidade da direção fazer com que todas as partes envolvidas no sistema de segurança estejam cientes e adequadamente instruídos sobre suas responsabilidades e papéis dentro da organização, bem como a motivação dessas partes no cumprimento dos termos de segurança com o desenvolvimento de programas de treinamento e a demonstração de apoio da própria direção às políticas de segurança, servindo de exemplo para todas as partes envolvidas. É necessária a existência de um processo disciplinar formal implementado e comunicado para as ações que devem ser tomadas em caso de violação de segurança, também é preciso definir um período de confidencialidade após o encerramento ou mudança de contratação.

4.2.4. Seção 8, sobre gestão de ativos.

Na seção 8, acerca da gestão de ativos, traz especificações sobre o inventário, os proprietários e o uso aceitável dos ativos. No inventário, todo e qualquer ativo que seja relevante no ciclo de vida da informação deve ser documentado e mantido, assim como a sua importância. O proprietário dos ativos é a pessoa ou entidade que tem responsabilidades para qualificar o ciclo de vida do ativo, a atribuição deve ser feita no momento de criação do ativo e o proprietário é o responsável pelo gerenciamento do ativo. Assim como, também, o uso aceitável dos ativos deve ser documentado e implementado. Após o encerramento de atividades, os ativos que estejam em posse de funcionários devem ser devolvidos.

“Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidades e criticidade para evitar modificação ou divulgação não autorizada”, [ABNT NBR ISO/IEC 27002:2013]. As informações devem ser classificadas de acordo com as necessidades de negócio para compartilhar ou restringir a informação, também é necessário classificar os ativos de acordo com a classificação da informação que será manuseada, armazenada, processada ou protegida pelo ativo. A classificação aplicada à informação deve ser analisada e atualizada de tempo em tempo, pois, algumas informações podem mudar de valor dentro da organização, por exemplo, uma informação que se torna pública não pode mais receber o mesmo tratamento de uma informação confidencial.

A partir da classificação da informação, é necessário criar um rótulo de tratamento da informação para que o manuseio da informação e de seus ativos seja feito baseado em um conjunto de procedimentos. A classificação e rotulação da informação são o que definem, por exemplo, com quem a informação deve ser compartilhada, mas também tem seus efeitos

negativos, de acordo com a sua classificação, um ativo ou informação pode ser identificada com mais facilidade por quem planeja roubá-la.

4.2.5. Seção 9, sobre controle de acesso.

Na seção nove da norma são especificados os requisitos de controle de acesso à informação, é necessário estabelecer uma política de controle baseada nos requisitos de segurança da informação, a norma especifica alguns itens que devem ser levados em consideração para a implementação da política de controle de acesso como os requisitos de aplicações, princípios de autorização da informação, consistência entre direito de acesso e políticas de classificação de informação, a legislação pertinente, a segregação de funções de controle de acesso como pedido de acesso, autorização e administração, arquivos de registro de eventos significantes e regras para acesso privilegiado.

Segundo a norma, há dois princípios que orientam a política de controle de acesso: necessidade de conhecer e necessidade de uso. No primeiro requisito a permissão de acesso somente pode ser dada para aquele que necessita da informação para realizar suas tarefas, já no segundo é dada a permissão de acessar os recursos de processamento da informação. Também é preciso inserir na política diretrizes de acesso à serviços de rede e à rede em si, procedimentos de autorização para determinar o acesso nos serviços de redes, determinar os requisitos de autenticação de usuários para monitorar o que é feito na rede.

Para o gerenciamento de acesso de usuário é necessário a criação de uma ID de acesso exclusiva para cada usuário para o gerenciamento das suas ações dentro da rede, a qual deve ser removida do sistema imediatamente caso o usuário deixe a organização. Um processo formal de provisionamento deve ser implementado para gerenciar os direitos de acesso de cada usuário, observando que os acessos permitidos estejam de acordo com as suas necessidades de uso e que não ultrapassam seu campo de trabalho dando acesso à áreas que não condizem com o seu setor.

O direito de acesso privilegiado deve ser controlado, é necessário especificar os campos a que o usuário terá acesso de forma privilegiada e definir um tempo de expiração para o privilégio e deve ser criada uma ID para este acesso, diferente da ID que o usuário utiliza para suas tarefas normais. O acesso privilegiado deve ceder direitos conforme a necessidade de uso, com base nos requisitos mínimos para a realização da tarefa. Os direitos de acesso devem ser analisados criticamente e regularmente, principalmente quando as funções ou cargo do usuário mudam dentro da organização.

Ao ceder direito de acesso à informação, o usuário detentor deste direito se torna responsável pela informação, portanto, convém que este seja orientado a seguir as práticas de uso da informação. Para o controle de acesso ao sistema e aplicações é necessário estabelecer quais informações e funções do sistema podem ser acessados de acordo com a política de controle de acesso, o procedimento de entrada no sistema deve ser seguro com uma técnica de autenticação adequada para validar a identificação do usuário e métodos alternativos para a verificação de senhas.

Os procedimentos de entrada no sistema devem proteger contra tentativas forçadas de entrada, validar as informações somente quando todos os dados forem informados, registre as tentativas de acesso, tanto frustradas quanto as bem sucedidas, faça comunicações de segurança em casos de suspeita de violação ou tentativa de acesso mal sucedido, registre data e horários de qualquer acesso, encerre automaticamente sessões inativas após um período definido de tempo.

Também é preciso criar um sistema de gerenciamento de senhas eficiente, que sejam interativos e assegurem senhas de qualidade, o sistema pode obrigar que o usuário utilize símbolos e números, assim como letras maiúsculas e minúsculas para tornar as senhas mais fortes, pode ser necessária também a mudança de senha após determinado período e mantenha um registro de senhas utilizadas anteriormente, impedindo que sejam usadas novamente. O acesso ao código fonte de programas e aplicações também deve ser protegido, de acesso restrito, para evitar alterações que insiram funcionalidade não autorizada ao sistema.

4.2.6. Seção 10, sobre criptografia.

Para garantir a autenticidade, integridade e confidencialidade da informação é indicado o uso de criptografia, que também precisa ter uma política de uso de controles criptográficos. É necessário avaliar o nível de proteção que a informação requer baseado em uma avaliação de riscos. Ao utilizar a criptografia, é necessário implementar um sistema de gerenciamento para proteger as chaves e recuperar as informações criptografadas caso a chave seja perdida, comprometida ou danificada.

“Convém que sejam consideradas na implementação da política criptográfica da organização as leis ou regulamentos e restrições nacionais aplicáveis ao uso de técnicas criptográficas, nas diferentes partes do mundo, e as questões relativas ao fluxo transfronteiras de informações cifradas”, [ABNT NBR ISO/IEC 27002:2013]. As técnicas criptográficas podem ser vistas, não apenas como métodos de segurança, mas também como ferramentas para

alcançar objetivos na organização como a confidencialidade, integridade e autenticidade da informação.

As chaves criptográficas em si também precisam de um sistema de gerenciamento que vai auxiliar a empresa a lidar de forma adequada com as chaves, especificando, por exemplo, requisitos na política de segurança da organização que irão definir aspectos como armazenamento, arquivo, recuperação, distribuição ou destruição das chaves, quais algoritmos criptográficos e tamanhos de chaves serão usados e um sistema que garanta a proteção da chave contra perdas ou modificação não autorizada, assim como alertas em caso de comprometimento da chave e meios de recuperação de chaves perdidas. “A gestão de chaves criptográficas é essencial para o uso eficaz de técnicas criptográficas”. [ABNT NBR ISO/IEC 27002:2013].

4.2.7. Seção 11, sobre segurança física e do ambiente.

Além de manter a informação segura, juntamente com todos os recursos lógicos que fazem parte do ciclo da informação, também é preciso assegurar os recursos físicos em que a informação está inserida ou é manipulada. As áreas de segurança devem ser muito bem definidas, a localização e capacidade de resistência do perímetro deve ser definido de acordo com os requisitos de segurança. Dependendo do quanto a informação é valiosa para a empresa, é necessário investir em meios físicos de segurança, como paredes robustas, portas adequadamente protegidas com barras, alarmes, fechaduras, meios de controle de acesso ao local, sistemas de prevenção contra incêndios, dentre outras medidas de segurança. Pode-se aplicar múltiplas barreiras de proteção ao redor das instalações, “o uso de barreiras múltiplas proporciona uma proteção adicional, uma vez que neste caso, a falha de uma das barreiras não significa que a segurança fique comprometida imediatamente”, [ABNT NBR ISO/IEC 27002:2013].

Apenas pessoas autorizadas devem ter acesso à área onde se encontra os equipamentos, este acesso deve ser monitorado e registrado com data e hora de acesso, além de um sistema de autenticação de identidade, um registro de todos os acessos deve ser mantido. Além de manter a segurança contra acesso indevido, é necessário assegurar que as instalações e os equipamentos estejam protegidos contra desastres naturais ou acidentes e que seja definido, previamente, meios de lidar com esses ocorridos assim como meios para evitá-los. No geral, todo e qualquer ativo que esteja dentro ou fora da organização deve estar inserido nas políticas de segurança.

4.2.8. Seção 12 e 13, sobre segurança nas operações e nas comunicações.

Assim como é necessário garantir a segurança dos equipamentos que fazem parte da vida da informação, também é preciso gerenciar a maneira que esses ativos são utilizados. Os procedimentos e as responsabilidades devem ser definidos pela gestão, incluindo gerenciamento de serviços terceirizados e planejamento de recursos para minimizar os riscos. As principais práticas citadas nesta etapa são referentes às atividades do dia-a-dia da empresa como inicialização e desligamento de computadores, geração de cópias de segurança, manutenção dos equipamentos, assim como a segurança e gestão das salas onde estes estão inseridos e o tratamento de mídias.

Para garantir a segurança das operações, alguns ambientes devem ser separados entre si, como ambientes de teste, desenvolvimento e produção, para diminuir os riscos de acesso indevido ou de modificações não autorizadas. “As atividades de desenvolvimento e teste podem causar sérios problemas, como, por exemplo, modificações inesperadas em arquivos ou no ambiente dos sistemas, ou falhas de sistemas. Nesse caso, é necessária a manutenção de um ambiente conhecido e estável, no qual possam ser executados testes significativos e que seja capaz de prevenir o acesso indevido do pessoal de desenvolvimento ao ambiente operacional”, [ABNT NBR ISO/IEC 27002:2013]. Todas as operações devem ser documentadas, além de haver um registro de atividades dos usuários do sistema que deve ser analisado criticamente em intervalos regulares.

4.2.9. Seções 14 e 15, sobre aquisição, desenvolvimento e manutenção de sistemas e o relacionamento na cadeia de suprimentos.

O principal objetivo deste trecho da norma é garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação. Todas as regras de desenvolvimento devem ser estabelecidas e aplicadas dentro da organização, “Desenvolvimento seguro é um requisito para construir um serviço, uma arquitetura, um software e um sistema seguro”, [ISO 27002], a produção de sistemas terceirizados também deve ser supervisionada.

Ativos que são acessados por fornecedores devem ser protegidos, requisitos de acesso devem ser definidos, acordados e documentados, a fim de reduzir riscos. A entrega de serviços também deve ser monitorada, analisada criticamente e validada pela organização.

1.2.9. Seção 16, sobre gestão de incidentes.

Procedimentos devem ser estabelecidos para assegurar a resposta rápida e eficiente em casos de incidentes. A organização deve manter um histórico de casos onde cada imprevisto é documentado, desde a sua causa até a solução, tudo deve ser analisado posteriormente e medidas devem ser tomadas para garantir a não ocorrência do mesmo episódio, diminuindo assim riscos futuros. Funcionários e terceiros devem estar cientes dos procedimentos de notificação destes eventos, para que a empresa possa fazer a correção o mais rápido possível.

Não apenas incidentes devem ser comunicados à organização, como também novas falhas de segurança casualmente encontradas devem ser reportadas imediatamente.

5. Principais tipos de ataques.

Diariamente empresas e organizações estão sujeitas a ataques aos seus dados e sistemas, não importa o seu tamanho, se uma empresa, mesmo de pequeno porte, utiliza serviços de TI, estará sujeita a ataques. Os principais ataques sofridos pelas organizações têm como objetivo o roubo ou sequestro de informações e dados que podem ter diversas utilidades, dependendo do objetivo final do autor do ataque. Nesta seção é apresentado uma lista de ataques mais comuns contra a Segurança da Informação e como eles funcionam.

5.1. Spywares.

Como o próprio nome já diz, spywares são programas espiões, têm como principal objetivo monitorar secretamente tudo que é feito no dispositivo. O vírus coleta informações sobre o usuário e seus hábitos de uso do dispositivo e da internet, isto inclui captura de pressionamento de tecla, captura de tela, credenciais de autenticação, endereço de email, dados de formulário de rede, informações sobre o uso de internet e outras informações pessoais.

O vírus atua de forma silenciosa no computador, sendo executado em segundo plano, e mesmo que o usuário descubra a presença do vírus, ele não vem com um recurso de desinstalação fácil. Normalmente o spyware pode infectar o sistema da mesma maneira que outros malwares fazem, através de um trojan, um vírus worm, exploit e outros tipos de infecção.

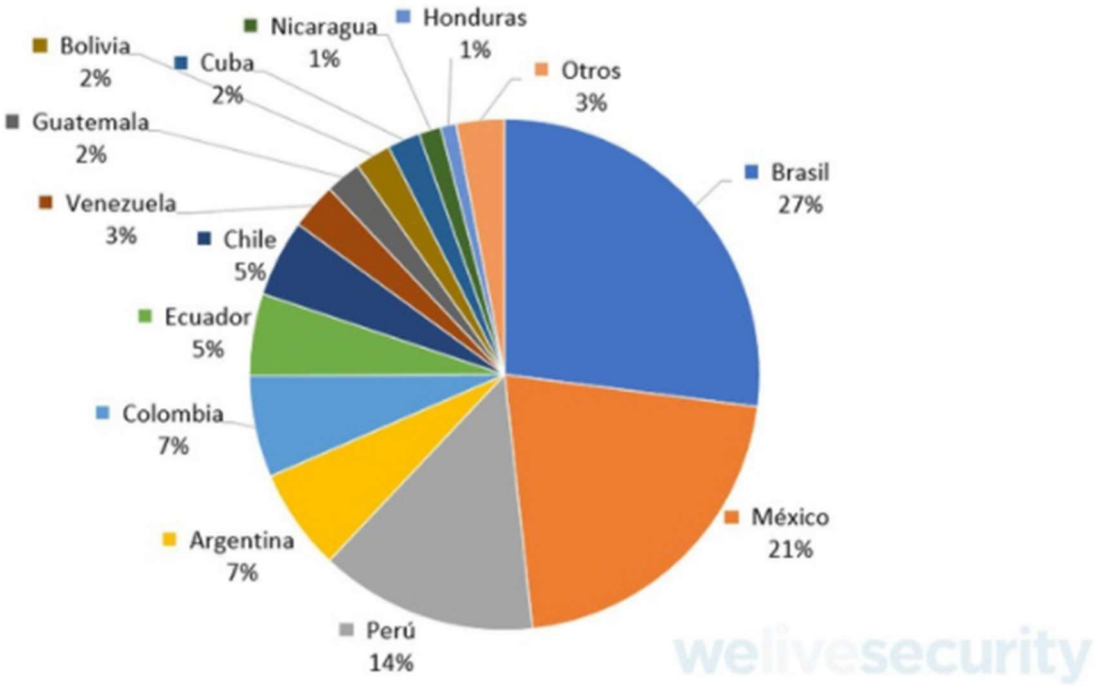
Existem muitas maneiras de um spyware infectar o computador, algumas delas são, vulnerabilidade na segurança do dispositivo, abertura de um email com um anexo de link desconhecido ou até mesmo visitando um website malicioso e visualizando uma página ou anúncio que resulte em um download do tipo drive-by, clicar em alguma parte da janela pop-up enganosa pode disparar uma infecção, ou até mesmo a troca de documentos com outro

dispositivo pode resultar no envio furtivo de um programa spyware infiltrado no arquivo, isto inclui instalador de programas, arquivos de música e documentos.

Os autores de spywares apresentam seus programas de forma disfarçada, como se fossem ferramentas úteis para o computador. Pode ser um acelerador de internet, um gerenciador de downloads, um limpador de disco rígido. Isto representa um enorme risco para o computador, pois mesmo que o programa seja desinstalado posteriormente, o vírus spyware continua atuando no dispositivo. As informações coletadas pelo programa são enviadas para um servidor específico controlado pela pessoa responsável pelo ataque.

Segundo a ESET, o Brasil é o país da América Latina mais afetado por essa ameaça, a maioria das infecções são genéricas, ou seja, não são voltadas especificamente ao nosso continente e sim spywares que se espalham pelo mundo todo, porém outras são códigos direcionados à América Latina. Na figura 3 pode-se observar que o Brasil lidera o ranking dos países com mais casos detectados.

Figura 3: distribuição de spyware por país, de setembro de 2018 a setembro de 2019



Fonte: welivesecurity.com.br

5.1.1 Tipos de spyware.

- **Programas de interceptação de senhas**

  São aplicativos projetados para capturar senhas em computadores infectados. As senhas coletadas podem incluir credenciais armazenadas em navegadores de rede, credenciais de login do sistema e diversas senhas críticas, os dados podem ser

armazenados na própria máquina, em um local escolhido pelo invasor, ou em um servidor remoto.

- **Trojans Bancários**

São aplicativos projetados especialmente para coletar credenciais de instituições financeiras. Se aproveitam da vulnerabilidade na segurança do navegador para modificar páginas de rede, conteúdo de transações ou inserir transações adicionais, tudo de maneira oculta tanto para o usuário quanto para o host de rede. Têm como alvo as instituições financeiras, incluindo bancos, corretoras, portais financeiros online ou carteiras digitais.

- **Infostealers**

São aplicativos que vasculham computadores infectados em busca de informações, incluindo nomes de usuário, senhas, endereços de email, histórico de navegadores, arquivos de registro, informações do sistema, documentos, planilhas e outros arquivos de mídia. Assim como o Banking Trojan, ele também pode se aproveitar da vulnerabilidade de navegadores para ter acesso a informações pessoais em serviços online e fóruns.

- **Keyloggers**

Também chamados de monitores do sistema, keyloggers são um tipo de spyware específico para registrar a atividade do computador. Isso significa que comandos específicos, senhas, histórico da web, todo texto digitado através do teclado, credenciais e orientações diversas são enviadas a um servidor remoto. Toda comunicação é espionada e ainda é possível capturar e transmitir imagens e vídeos de qualquer dispositivo conectado.

5.2. Ransomwares.

Quando se fala em segurança de dados, os ransomwares são a possibilidade mais assustadora. Eles criam um ataque complexo onde os dados de um computador, ou de uma rede inteira, são encriptados. Todas as informações de um ERP, por exemplo, podem ser encriptadas e transformadas em uma extensão inacessível. Para que os elementos possam ser acessados novamente é necessária uma chave de descriptografia que, normalmente, é oferecida por quem invade o dispositivo, em troca de um pagamento em bitcoin, que é uma moeda virtual de difícil rastreamento.

Assim como o spyware, o ransomware é de difícil detecção, ele ataca se disfarçando e, normalmente, o usuário só percebe que foi infectado quando todos os seus arquivos já estão bloqueados. Pode ser enviado por email através de um link suspeito ou estar presente em sites maliciosos, pode ser instalado junto com programas baixados em sites não confiáveis ou ser enviado como link em redes sociais, meio muito utilizado para propagar o vírus.

Em 2016 a Kaspersky Lab descobriu um ransomware brasileiro que emite uma janela parecida com um pedido de atualização de Adobe Flash Player. Quando o usuário clica no link para “atualizar”, o computador é infectado rapidamente e em pouco tempo sequestra os dados da vítima. Segundo a empresa que descobriu o vírus, a extorsão requerida pela devolução dos dados era de cerca de 2 mil reais em bitcoin.

Ainda em 2016, mais precisamente no mês de março, o FBI emitiu um alerta preocupado com o ransomware MSIL/Samas, sendo este um dos mais perigosos atualmente, pois ele tem a capacidade de infectar uma rede inteira de dispositivos, basta que apenas um dispositivo da rede seja infectado e o vírus se espalha. No mesmo ano a Palo Alto Networks, empresa especializada em segurança digital, descobriu o primeiro ransomware criado para sistemas Mac OS X. Na ocasião, o malware Key Ranger infectou algumas máquinas através do programa Transmission BitTorrent. Ele criptografou o disco rígido em três dias, agindo silenciosamente enquanto isso. Para solucionar o problema, a Transmission Project lançou a versão 2.92 do Transmission BitTorrent. De acordo com os desenvolvedores, a atualização remove os arquivos infectados do Mac.

Outro alerta foi emitido em 2020 pelo FBI, pelo Departamento de Saúde e Serviços Humanos (HHS) e pela Agência de Segurança Cibernética e de Infraestrutura de Segurança Interna (Cisa), segundo Alex Holden, da empresa de inteligência cibernética Hold Security, há uma discussão na dark web cujo objetivo é infectar mais de 400 hospitais e instalações médicas com a finalidade de abalar um dos sistemas mais necessários no momento em que vivemos uma pandemia.

A Microsoft tem em seu site uma página toda dedicada ao Ransomware e como se prevenir de um ataque desse tipo. Ter o firewall sempre ativado e os programas sempre atualizados são os primeiros passos para uma boa proteção. A preocupação com este tipo de malware é tão grande que algumas empresas de TI estão desenvolvendo soluções específicas. É o caso do Bitdefender Anti-Ransomware, um pequeno software que permanece ativo em segundo plano monitorando o sistema operacional. O programa age preventivamente e informa

ao usuário se alguma tentativa de invasão ocorrer. Outro produto disponível no mercado é o Malwarebytes Anti-Ransomware.

5.3. Backdoor.

Backdoor é um recurso usado por diversos malwares para garantir o acesso remoto do sistema ou rede infectada explorando falhas existentes em programas instalados, softwares desatualizados e firewall para abrir portas do roteador. Alguns backdoors podem ser explorados por sites maliciosos através de vulnerabilidades existentes nos navegadores para garantir o acesso parcial ou total do sistema, instalação de outros malwares ou roubo de dados.

É um dos ataques mais prejudiciais ao usuário, tanto quanto o ransomware. Além de ter acesso a todos os arquivos presentes no computador infectado, o invasor ainda pode controlar funções como ligar e desligar a webcam, microfones, drives de CD e teclado. Uma forma muito comum de infecção é a instalação de arquivos maliciosos do tipo Cavalo de Troia, que deixam o caminho livre para que o cracker consiga voltar e ter controle sobre a máquina sem passar por verificações de segurança.

Outra forma bastante comum é através da instalação de programas de acesso remoto com o TeamViewer e o NetBus. Quando instalados sem o consentimento do usuário ou mal configurados, podem também ser considerados Backdoors. Assim como a maioria das ameaças online, os backdoors também são propagados graças à inocência dos usuários. Recentemente foi descoberto que o computador da atriz Jennifer Lawrence, que teve fotos íntimas vazadas na internet em 2014, estava servindo de chamariz para instalar o Win32/Fynloski, um arquivo malicioso que tem como objetivo o roubo de dados além de dar acesso à máquina.

5.4. Ataque DoS e DDoS.

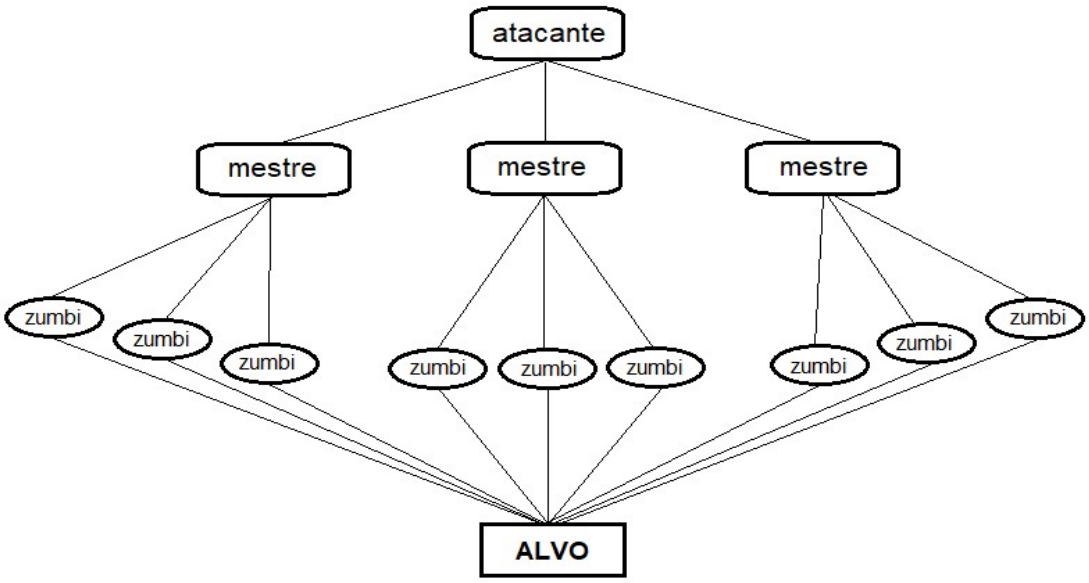
Diferente dos outros ataques onde o objetivo é o roubo de informações, dados e documentos, os ataques do tipo DoS (*Denial of Service*) e DDoS (*Distributed DoS*), também conhecidos como negação de serviço distribuído, tem como objetivo a queda de um servidor. Serviços de rede, como servidores web, possuem uma capacidade limitada para atender solicitações simultâneas, além disso, o canal que conecta o servidor à internet também tem uma largura de banda limitada e quem busca esse tipo de serviço pode escolher opções de acordo com a sua demanda.

O objetivo dos ataques DoS e DDoS é fazer com que um servidor atinja sua capacidade máxima, impedindo a prestação do serviço, por estar sobrecarregado. Durante o ataque são

enviados vários pacotes para causar uma sobrecarga no servidor e impedir o oferecimento dos seus serviços. É um tipo de ataque que não pode ser evitado, uma vez iniciado, não há como se proteger, a não ser desligar o servidor. “Esses ataques são baratos de conduzir e mais difícil de atribuir por causa de sua natureza distribuída, então, pessoas, organizações ou mesmo governos usam DDoS como uma forma de guerra cibernética para marcar sua dissidência”, .

Nos ataques do tipo DDoS o invasor controla uma ou mais máquinas mestras (botmaster) que se conectam a várias outras máquinas, denominadas *zumbis* (botnet), de maneira voluntária ou involuntária, como exemplificado na figura 4.

Figura 4: representação de uma ataque DDoS



Fonte: adaptado de infowester.com

A preferência para os mestres são máquinas que ficam conectadas à internet o tempo todo. Para conseguir a conexão involuntária, o atacante utiliza de falhas no sistema operacional, engenharia social, entre outras maneiras para criar os zumbis que atacam diretamente o servidor alvo, a quantidade de zumbis não é precisa e depende da capacidade do alvo, quanto maior a capacidade, mais zumbis são necessários para o sucesso do ataque. Para se ter uma noção da abrangência que este tipo de ataque pode alcançar, em 2016 mais de 100 mil máquinas foram infectadas para sobrecarregar o ISP - *Singapore Star Hub*, que é uma empresa líder local em soluções tecnológicas.

A diferença entre os ataques DoS e DDoS é a quantidade de máquinas utilizadas, enquanto o DDoS faz uso de várias máquinas, o DoS utiliza apenas uma para enviar os pacotes e é preciso ter uma conexão de banda larga e um computador capaz de fazer uma grande quantidade de envios de pacotes ao mesmo tempo. O DDoS é necessário quando o alvo tem uma grande capacidade, enquanto que, para servidores menores é utilizado o ataque DoS.

Existem duas categorias em que se pode classificar os ataques DDoS, falsificação de IP e IP de origem real. No primeiro os endereços IP de origem não representam máquinas reais, mas são gerados de maneira artificial. Este tipo de ataque é mais facilmente detectado por Sistemas de Detecção de Intrusão (IDS). Já a segunda categoria utiliza o IP real das máquinas infectadas, "o ataque DDoS baseado em dados reais dos endereços IP de origem geralmente utilizam nós comprometidos na Internet para lançar o ataque", [Fung e McCormick].

Não há métodos para evitar esse tipo de ataque, mas existem técnicas de mitigação que podem reduzir o dano causado, estas técnicas podem ser classificadas em dois grupos principais: capacidade e filtro. No primeiro grupo os processos têm seu tráfego de rede limitado usando uma abordagem baseada em prioridade, já no método de filtros o tráfego malicioso é identificado e bloqueado, liberando o acesso apenas para o tráfego considerado benigno. Os sistemas baseados em capacidade, normalmente ficam sobrecarregados durante um ataque, já os sistemas baseados em filtro possuem um processo de detecção de anomalias muito acurado e preciso, tanto que, mesmo se o sistema falhar, o fluxo falso-positivo é simplesmente bloqueado, [Fung e McCormick].

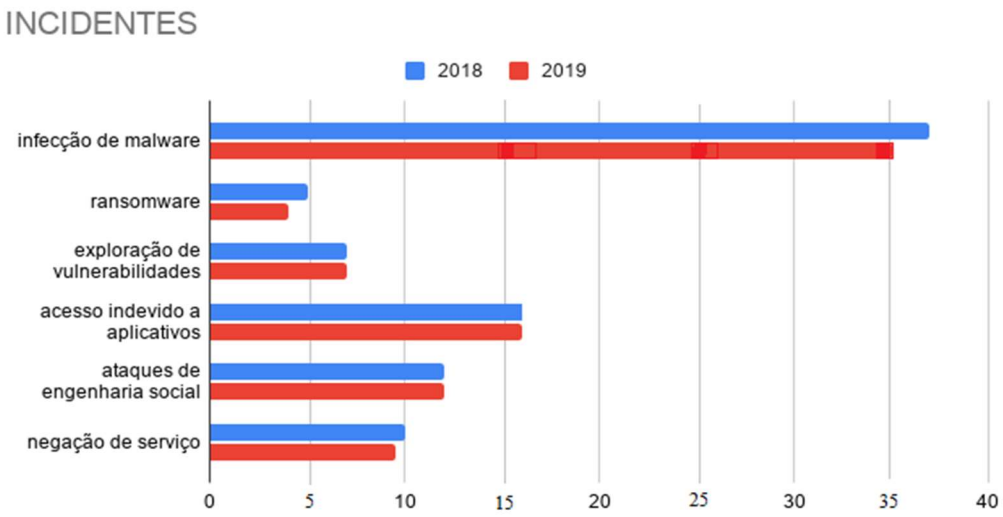
6. Problemas de Segurança da Informação

Os ataques no meio digital são a principal preocupação quando se fala de segurança da informação e em muitos casos a prevenção desses ataques se concentra em possuir meios tecnológicos de combate, porém poucas empresas consideram criar planos de continuidade de negócio relacionado à segurança, de acordo com o relatório ESET Security Report 2020, apenas 33% das quase quatro mil empresas entrevistadas em distintos eventos de segurança possuíam algum mecanismo para tratamento de ataques.

E, apesar da maioria dos incidentes de segurança ter relações com ataques diretos ao sistema, como malwares ou ransomwares, como mostrado na figura 5, poucas têm agido e criado formas eficientes de respostas a esses crimes, pensamento defendido por John Walker, professor da Universidade de Nottingham, na Inglaterra, durante o evento Cyber Security Summit Brasil de 2018, "A indústria de cibersegurança é ruim. As empresas têm dificuldades

ao tratar as ameaças hoje em dia. Resposta a incidentes é a chave e é algo que precisa ser planejado com antecedência", relata Walker.

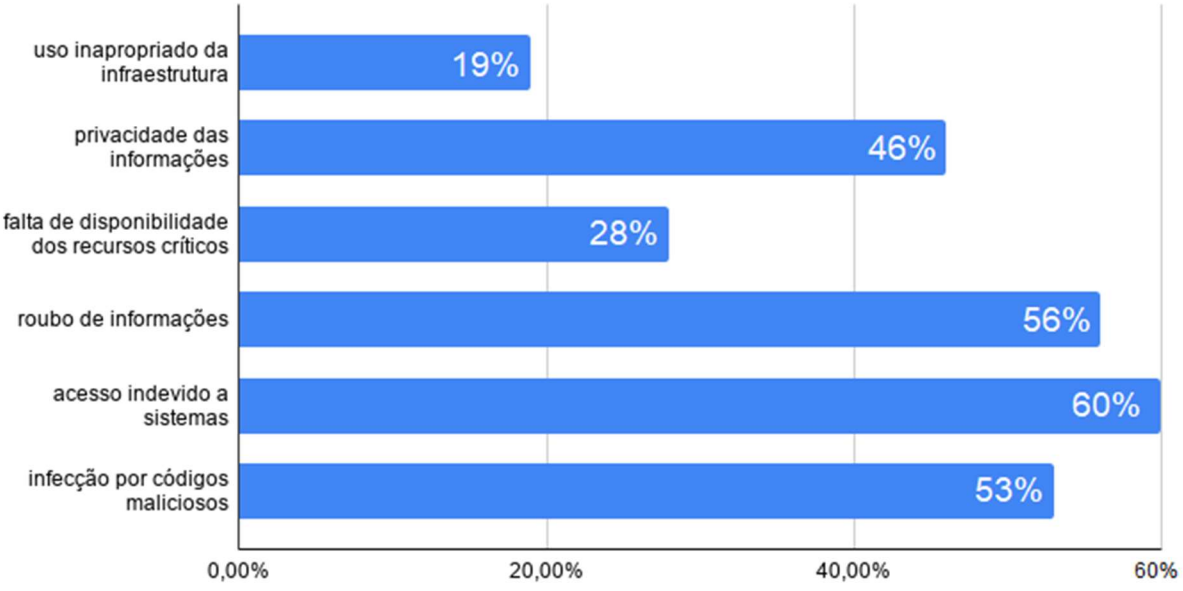
figura 5: incidentes relatados pelas empresas



fonte: adaptado de ESET Security Report América Latina 2020

Apesar do grande número de ataques por infecção de malware, o que também representa a maior preocupação das empresas, os ataques relacionados a atividades humanas não podem ser ignorados, pois representam uma parte bastante significativa do gráfico da figura 5. Já na figura 6, pode-se perceber para onde está voltada a atenção das organizações quando se fala de vulnerabilidades no sistema.

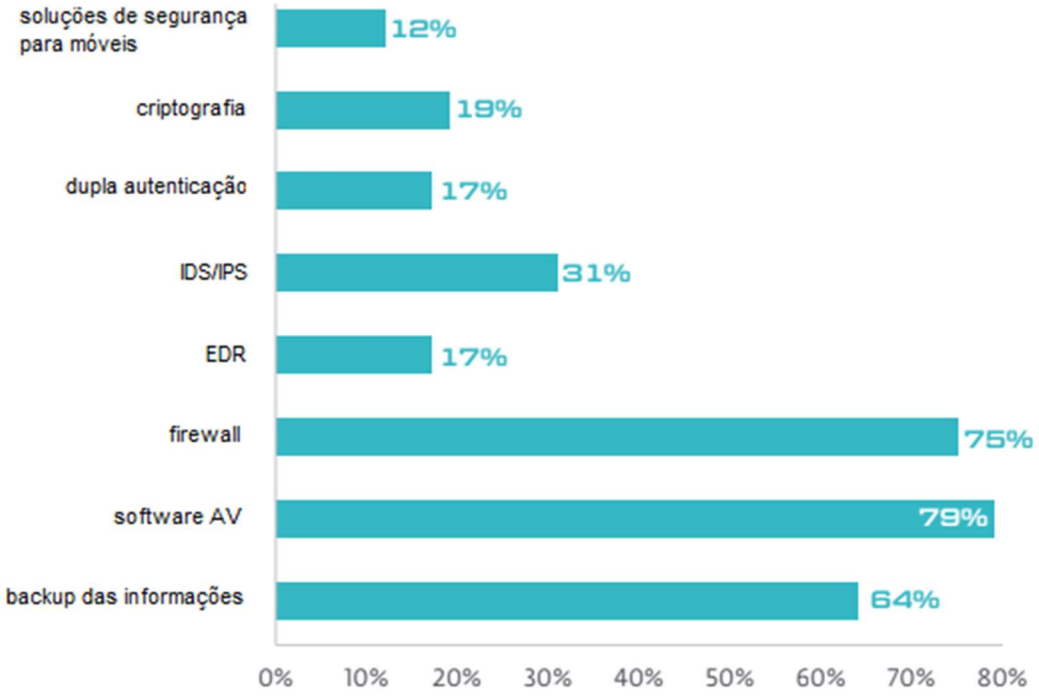
figura 6: preocupações relacionadas à segurança



fonte: adaptado de ESET Security Report América Latina 2020

Roubo de informações e acesso indevido ao sistema apresentam a maior porcentagem no gráfico da imagem 6, porém, em contrapartida, o uso inapropriado do sistema foi escolhido pelos entrevistados como o item menos preocupante, o que reflete a cultura da empresa em relação à segurança de dados. Na figura 7 pode-se observar as principais providências que as empresas tomam diante do cenário tecnológico.

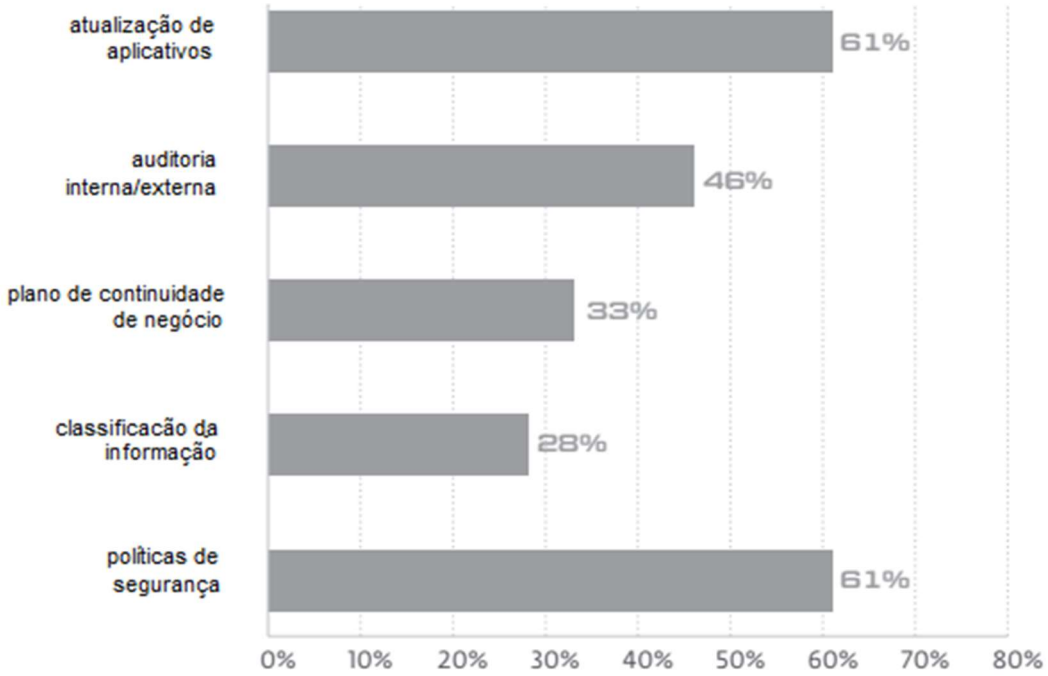
figura 7: controles baseados em tecnologia



fonte: ESET Security Report América Latina 2020

A maior parte dos controles baseados em tecnologia implementados pelas organizações são relativos a ataques de códigos maliciosos que podem afetar o sistema, na imagem 7 nota-se que apenas 12% das organizações entrevistadas possuem algum mecanismo de segurança física dos seus equipamentos e mesmo no uso de segurança lógica, é reduzido o número de empresas que usam mecanismos básicos de segurança como criptografia ou autenticação dupla.

figura 8: controles baseados em gestão



fonte: ESET Security Report América Latina 2020

Além do evidente desleixo em relação à ações humanas, que podem significar um grande risco ao sistema de uma empresa, na figura 8 pode-se observar que apenas uma parcela pequena possui plano de continuidade de negócio em caso de crises ou ataques, menor ainda a parcela cuja os dados são classificados, o que é de extrema importância dentro de uma organização.

6.1. Falta de uma política de segurança definida.

De acordo com a ESET, a principal preocupação das empresas é o acesso indevido à informação, seguido por roubo de informação e infecção por códigos maliciosos. Ainda assim, poucas empresas investem em um sistema de segurança adequado, não só em sistema, mas em definir estratégias para prevenir e tratar incidentes. “Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes” (norma ISO/IEC 27002).

É necessário que seja criado estratégias que envolvam todos os ativos que fazem parte da vida da informação como controle de acesso, segurança física e do ambiente, backups e criptografia. Tudo deve ser documentado e apresentado aos funcionários e quaisquer partes externas relevantes, é necessário que a organização faça entender a importância de seguir as

políticas de segurança e instruir funcionários sobre atividades decorrentes do dia-a-dia da organização que podem incidir sobre o sistema.

6.2. Obsolescência dos sistemas e ferramentas desatualizadas.

Algumas empresas, principalmente as que têm um perfil mais conservador, ainda se recusam ou têm dificuldades de adotar novas tecnologias, que são adequadas para proteger seus sistemas, tornando-os vulneráveis a ataques. Conforme os meios de ataques evoluem a tecnologia também se renova.

Softwares como antivírus e firewalls devem ser atualizados frequentemente, assim como os hardwares e o tratamento de incidentes, tudo deve ser renovado de acordo com o necessário. É importante que a organização tenha conhecimento sobre as ameaças às quais pode estar vulnerável e se atualize sobre novos meios de ataques que surgem com o tempo.

6.3. Falta de treinamento para lidar com os sistemas.

Quando se fala de segurança da informação, muitas empresas tendem a pensar que a responsabilidade é apenas do gerente de TI, porém toda e qualquer que utiliza o sistema da organização precisa ser orientada sobre o básico para assegurar a organização contra ataques. “A principal ameaça para qualquer segurança é o próprio ser humano, pois todo processo de segurança se inicia e termina no usuário do sistema”, Santos (2011).

É importante fazer parte da cultura da empresa um comportamento consciente do domínio da informação a fim de evitar riscos ou perdas. “Para reduzir os riscos relacionados a erros humanos ou atos criminosos por parte dos usuários internos, é aconselhável que a organização estabeleça políticas de informação, controles e procedimentos enfocando a área de pessoal”, Aramuri e Maia (2018). É preciso que haja o controle das atividades, treinamento, supervisão, segregação de funções e políticas adequadas para o uso da informação, tudo deve ser monitorado e atualizado frequentemente a fim de prevenir incidentes.

7. A Segurança da Informação no mundo atual

O Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (National Institute of Standards and Technology-NIST) descreve risco como uma função da probabilidade de uma determinada fonte de ameaça exercer qualquer vulnerabilidade potencial e o impacto resultante desse evento adverso na organização. Em um cenário pandêmico, onde o trabalho remoto e aulas EAD (ensino à distância) se tornaram parte da rotina de milhões de pessoas pelo mundo todo, criminosos veem a oportunidade perfeita para aplicar suas técnicas. Antes da pandemia,

a maioria dos casos de ataques digitais no Brasil aconteciam na forma de exploits, que tentam tirar vantagens de vulnerabilidades do sistema.

Porém, com o aumento do número de dispositivos sendo utilizados em casa por pessoas, muitas vezes, leigas no quesito segurança, a estratégia de ataques foi adaptada para tentar enganar esse público. Segundo o FortiGuard Labs, criminosos utilizam de e-mails, links de sites e até mensagens telefônicas contendo anexos de phishing maliciosos, tudo sobre o pretexto de pandemia da COVID - 19, “em abril ocorreu o maior número de campanhas de phishing por e-mail relacionados à covid-19, foram mais de 4.250. O maior pico ocorreu em 2 de abril, quando a Fortinet relatou 330 campanhas com e-mails maliciosos com o tema ‘covid-19’ em todo o mundo. Os números têm diminuído constantemente desde abril, com 3.590 campanhas de phishing por e-mail em maio e 2.841 em junho”, relata Bonatti.

O problema da epidemia atual acende nas empresas a necessidade de implementar protocolos de segurança para gerenciar acesso, processo e armazenamento de informações e de educar seus funcionários quanto a importância de seguir essas normas. Segundo Leonardo Lemes, diretor de segurança cibernética na Service IT, algumas medidas que podem ser tomadas por uma organização para a realização de trabalho remoto são: (1) provisão de equipamento adequado para o funcionário, (2) especificação de métodos de acesso seguros, (3) monitoramento de segurança, (4) segurança física do equipamento, (5) procedimentos para cópias e backups, (6) devolução do equipamento quando se encerrarem as atividades remotas e (7) provisão de suporte e manutenção dos equipamentos. Outras orientações que também devem ser observadas são sobre o uso e acesso ao equipamento e informações por familiares ou visitantes.

Além de emails maliciosos, outra ferramenta que tem ganhado espaço dentro das organizações é a chamada Machine Learning (ML), que é muito utilizada para simplificar tarefas através da sua aprendizagem automática. É utilizada em trabalhos longos como análises de uma grande quantidade de dados, até realizar tarefas repetitivas. Porém o ML têm sido alvo de engenharia social, de acordo com o relatório de tendências 2020 da ESET Security “em 2019 o ML ganhou notoriedade devido a outro assunto preocupante: o aumento das *deepfakes*. Esta tecnologia que faz com que o ditado popular ‘ver para crer’ perca todo o sentido, pode ser aproveitada para prejudicar a reputação de figuras públicas ou até de influir na opinião pública”.

Em março de 2019 o Wall Street Journal publicou um caso onde criminosos utilizaram de inteligência artificial para imitar a voz do CEO de uma empresa alemã de energia que pedia uma transferência de € 220.000 (cerca de R$ 1.4 milhões) a um fornecedor húngaro, destacando

a urgência da operação e exigindo o pagamento em até uma hora. A empresa não teve seu nome revelado, apenas o caso foi divulgado pela seguradora Euler Hermes Group SA, responsável por cobrir o valor total roubado.

Sendo a tecnologia, aliada de qualquer organização, independente do seu tamanho, os alvos de ataques vêm se diversificando cada vez mais. Além do crescente número de incidentes relacionados a computadores pessoais, hotéis têm sido alvos de ataques, pelo fato de reunir informações de muitas pessoas em um só lugar, os dados obtidos são desde nomes completos até dados de cartões de créditos.

Grandes redes hoteleiras têm sido alvo desses ataques como a Marriot International que anunciou em março de 2020 que informações de mais de 5 milhões de hóspedes foram acessadas indevidamente, a rede de hotéis está presente em mais de 131 países, incluindo o Brasil. Outra grande rede afetada foi a MGM Resorts International, onde a violação afetou mais de 10 milhões de hóspedes. Grandes empresas da área têm sido alvo desses ataques justamente por ser um setor não focado em tecnologia, mas que reúne informações valiosas.

Além dos ataques a bancos de dados, sites de hotéis vazam dados pessoais, segundo a Symantec, em um teste feito em sites de 1500 hotéis de 54 países, 67%, ou seja, dois terços desses sites têm problemas de privacidade, o que resulta no vazamento de informações. O setor hoteleiro é apenas uma pequena parte do grande ramo de organizações ao redor do mundo que sofrem com ataques e invasões, e por não fazer parte do setor tecnológico estão mais vulneráveis à falhas.

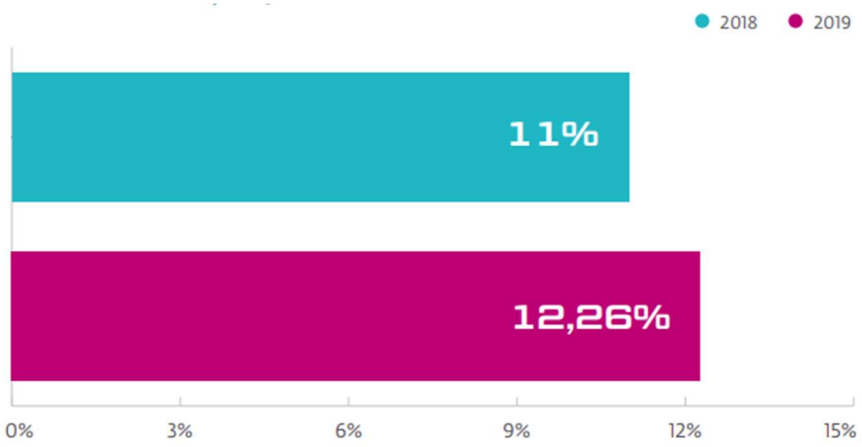
A maioria dos incidentes de segurança da informação ainda ocorre em empresas atuantes no meio da tecnologia, segundo o relatório ESET, 60% das empresas sofreram algum incidente em 2019, número que se manteve em 2020, conforme mostrado na figura 9.

Figura 9: porcentagem de empresas com registro de incidentes em cada país da América Latina

Fonte: ESET Security Report

Dentro das informações coletadas acerca dos incidentes, 32% são por infecção de códigos maliciosos. No que diz respeito a ransomwares, uma variante de malware, o cenário é decrescente a cada ano na américa latina, apresentando um índice de 18% em 2017, 8% em 2018 e 6% em 2019. Por outro lado, no Brasil foi registrado um crescimento desse tipo de ataque em 1,26% em relação ao ano anterior, passando de 11% em 2018 para 12,26% em 2019, como pode-se observar na figura 10.

figura 10: infecções por ransomware no Brasil



Fonte: ESET Security Report

Uma atenção especial deve ser dada ao setor bancário, principalmente no Brasil, que tem se tornado um dos principais alvos de trojans, utilizados para roubar informações financeiras. Segundo a ESET, somente entre os meses de janeiro e abril de 2019 houveram 58,3 mil casos de infecção, assumindo a primeira posição com folga, em segundo lugar vem o Chile com 5,1 mil casos registrados no mesmo ano.

Segundo Silva (2019), no Brasil é muito comum o uso de engenharia social para enganar pessoas, fazendo com que acessem links maliciosos, páginas que são cópias dos sites oficiais de bancos, e até mensagens sms ou ligações. Já para o exterior, criminosos brasileiros estão focando no uso de trojans, este ano (2020) a empresa Kaspersky confirmou quatro famílias de malwares de origem brasileira atuando na Europa e na América Latina, os criminosos responsáveis também demonstraram interesse na América do Norte e China. A tendência de ataques foi nomeada de The Tetrade e fazem parte dessa família grandes trojans já conhecidos como Guildma, Javali, Melcoz e Grandoreiro, os responsáveis se beneficiam do fato de muitos Bancos operantes no Brasil também atuam em outros países.

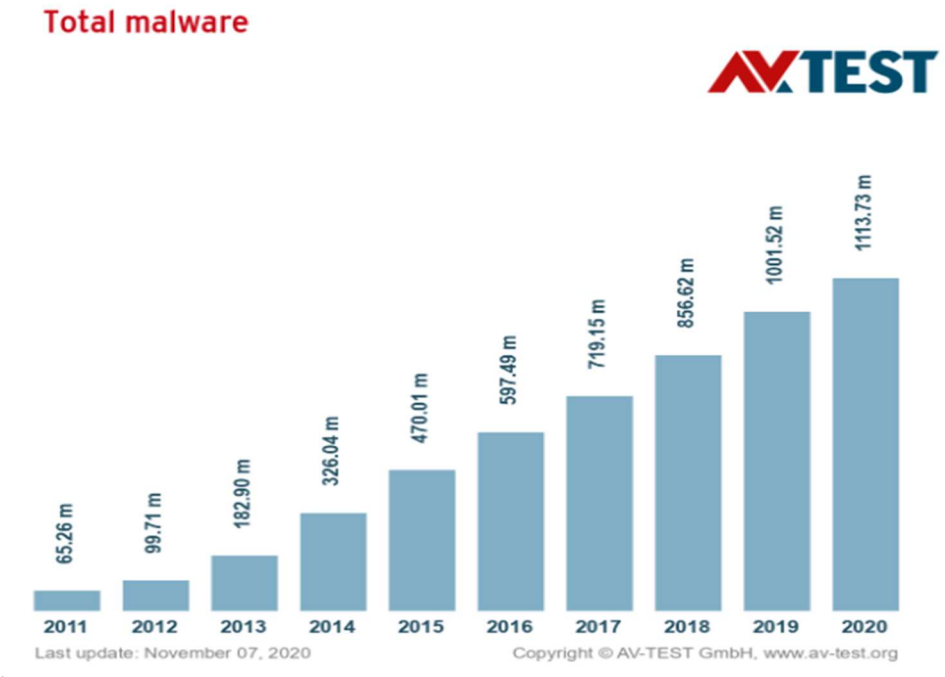
“Os criminosos brasileiros estão criando rapidamente um ecossistema de afiliados, recrutando cibercriminosos para trabalhar em outros países, adotando o MaaS (malware como serviço) e adicionando rapidamente novas técnicas ao malware como forma de mantê-lo relevante e financeiramente atraente para seus parceiros”, [Kaspersky]. É provável que essas ameaças evoluam para atingir outros países e continentes e certamente estão liderando esse tipo de ataque na América Latina, buscando parceiros locais para ajudar na administração do dinheiro roubado e na tradução.

7.1. Criação de novas ameaças

Quando os dados eram guardados em papéis, era necessário, basicamente, algumas caixas e uma sala bem trancada para garantir a segurança das informações. Porém, atualmente, com a incorporação dos trabalhos remotos e dispositivos pessoais que se organizam de forma distribuída em redes, o tratamento da informação se torna muito mais complexo. “A segurança no meio cibernético é um conjunto de tecnologias e processos projetados para proteger computadores, redes, programas e dados de ataques, danos ou acesso não autorizados”, [Sarker et al. J Big Data, 2020].

Devido à crescente dependência dos meios digitais, diversos incidentes como malwares, negação de serviço, phishing, dentre outros, também crescem de forma exponencial. De acordo com o instituto alemão AV-TEST, em 2011 haviam 65 milhões de malwares conhecidos pela comunidade de segurança, em 2016 esse número chegava a quase 600 milhões e em 2020 ultrapassou a marca de 1 bilhão de programas maliciosos registrados, tendo uma média de 350 mil novos softwares e aplicativos potencialmente indesejados (PUA) identificados por dia pelas suas ferramentas de análise, como mostrado na figura 11.

figura 11: total de novos malwares registrados na última década

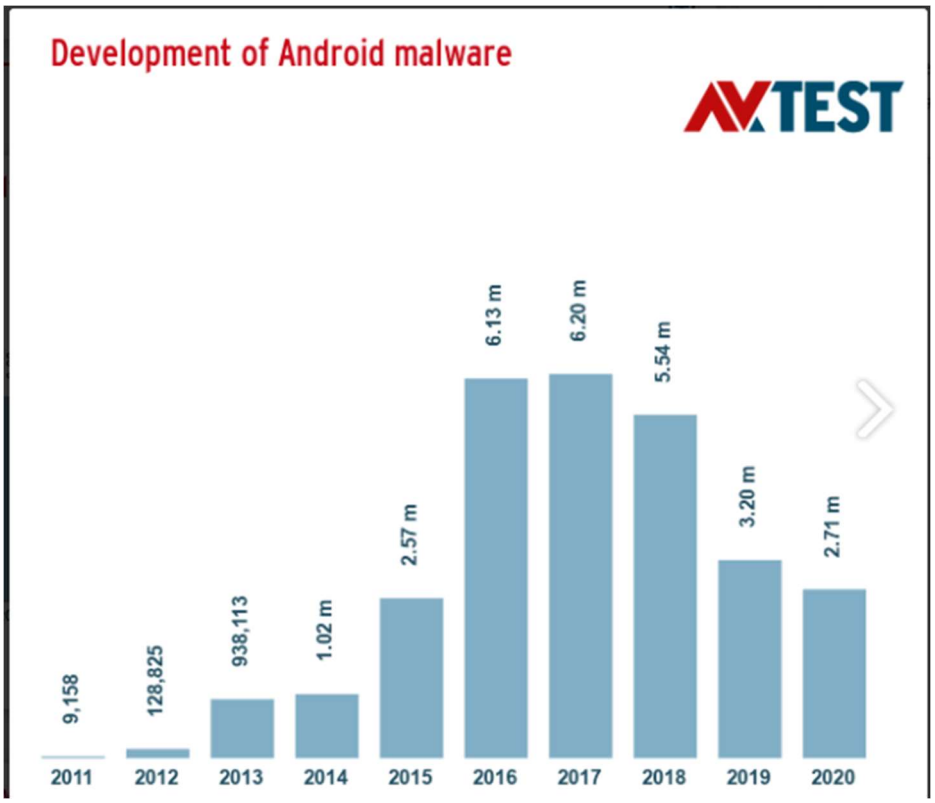


fonte: AV-TEST, disponível em www.av-test.org.

E essa crescente onda de ataques tem atingido não só computadores, como também dispositivos Android. Com a chama atraente de acesso a ilimitados serviços na palma da mão, incluindo serviços essenciais como banking ou cartões de créditos, a quantidade de dispositivos aumenta cada vez mais a cada ano, assim como cresce o interesse de criminosos em cima das

plataformas móveis. Em uma década o desenvolvimento malwares para android passou de 9 mil em 2011 para quase 3 milhões em 2020, como pode-se observar na figura 12.

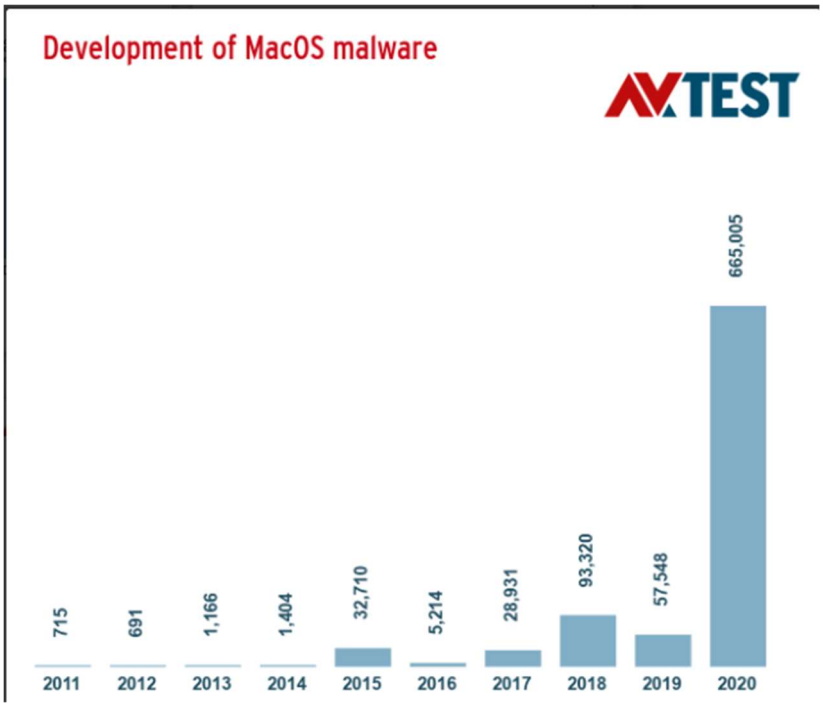
figura 12: desenvolvimento de malwares para android



fonte: AV-TEST, disponível em www.av-test.org.

Não só o Android tem chamado mais a atenção de criminosos, como também o sistema operacional da empresa Apple. A popularização da marca, que atualmente é símbolo de desejo, fez com que a empresa registrasse no segundo trimestre de 2020 um lucro de 11% a mais do que em 2019, indicando um aumento histórico nas vendas. E como o esperado, a atenção de criminosos para o sistema operacional MacOS também teve um aumento histórico em apenas 1 ano, passando de 57 mil malwares registrados em 2019 para mais de 600 mil softwares maliciosos em 2020, como observa-se na figura 13.

figura 13: desenvolvimento de malwares para MacOS



fonte: AV-TEST, disponível em www.av-test.org.

A capacidade de identificar e eliminar ameaças em tempo hábil é um dos principais objetivos da segurança da informação, um sistema que não está devidamente preparado para lidar com novos incidentes não é eficaz. Por conta disso, cada vez mais organizações têm investido em meios de identificar previamente ou eliminar de maneira rápida novos ataques.

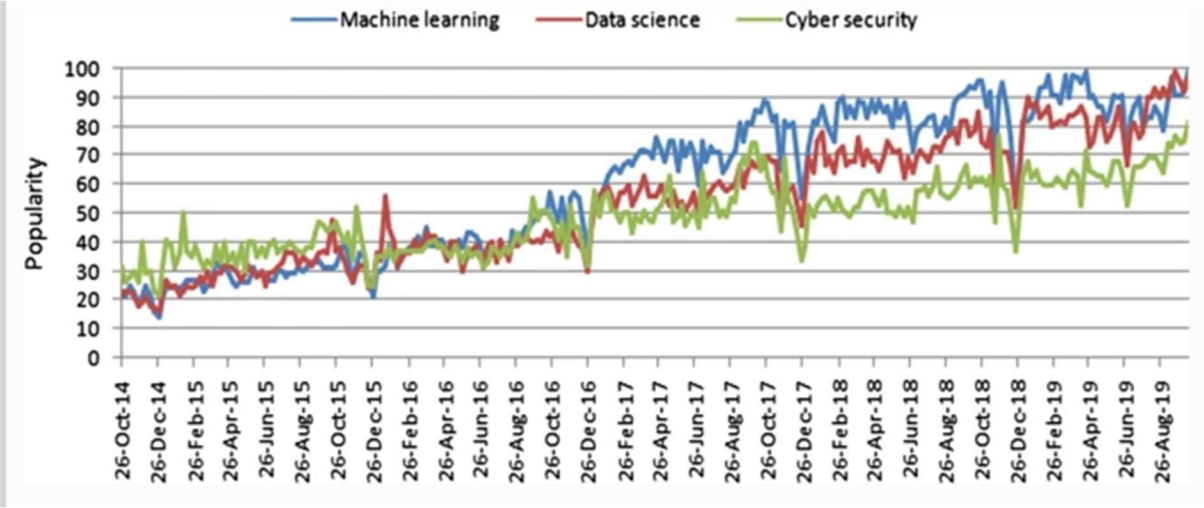
Nos tempos atuais, a segurança da informação está passando por mudanças tecnológicas e operacionais onde a ciência de dados (Data Science) opera como principal impulsionador desta mudança, o aprendizado de máquina (Machine Learning), uma parte essencial da Inteligência Artificial (IA) pode desempenhar um papel essencial para descobrir as percepções dos dados, "O aprendizado de máquina pode mudar significativamente o panorama da segurança cibernética e a ciência de dados está liderando um novo paradigma científico", [Sarker, 2020].

Cada vez mais os dados são vistos como patrimônio das organizações, até mesmo pequenas empresas têm se atentado à importância das informações, não apenas como produtos utilizados no dia-a-dia, como também algo fundamental para planejamentos futuros. Porém, o avanço tecnológico voltado para a segurança não tem acompanhado muito bem o fluxo de novos ataques, Segundo Larry Ponemon, presidente e fundador do Ponemon Institute, "mais da metade dos profissionais de segurança cibernética afirmam que suas organizações são ineficazes em impedir as principais ameaças porque suas soluções de segurança não são eficazes na detecção de ataques avançados".

O Ponemon Institute realizou uma entrevista com 671 profissionais de segurança de TI responsáveis por gerenciar e reduzir o risco de segurança de sua organização. As organizações entrevistadas estão muito preocupadas com o aumento significativo de ameaças novas e desconhecidas contra suas empresas (um aumento de 69% dos entrevistados em 2017 para 73% em 2019).

Uma das alternativas para resolver este problema e que vem sendo um dos principais focos de desenvolvimento é o uso de inteligência artificial, mais especificamente, machine learning. Aprendizado de máquina (ML), ciência de dados (DS) e cibersegurança (CS), essas tecnologias relacionadas têm se popularizado ao longo dos anos, como pode-se observar na figura 14.

figura 14: tendência de popularidade



fonte: Google Trends

ML já é bastante utilizado em diversas áreas como medicina, processamento de imagens, dentre outros, pela capacidade de analisar grandes quantidades de dados e definir ações com base nessa análise. Uma das modalidades de aprendizagem de máquina é o Deep Learning, segundo NSCAI Intern Report for Congress (2019), “DL é uma técnica estatística que explora grandes quantidades de dados como conjuntos de treinamento para uma rede com várias camadas ocultas, chamada de rede neural profunda, onde é treinado em um conjunto de dados, gerando saídas, calculando erros e ajustando seus parâmetros internos. Em seguida, o processo é repetido centenas de milhares de vezes até que a rede atinja um nível aceitável de desempenho”.

Devido à importância de se identificar um ataque de forma rápida, a inteligência artificial de aprendizado tem sido implementada para fazer análises de tráfego e reconhecer anomalias maliciosas na rede. Para isso, é muito importante selecionar dados de alta qualidade,

“Usar dados de alta qualidade no Deep Learning é tão importante quanto usar arquiteturas de rede neural profunda bem estruturadas. Ou seja, a obtenção de dados de qualidade deve ser uma etapa importante, que não deve ser ignorada, mesmo na resolução de problemas de segurança usando Deep Learning”, [Choi et al. 2020]. Além da qualidade dos dados, a definição do problema também precisa de atenção, “é crucial ter uma imagem clara de qual problema um sistema visa: quais são especificamente os ataques a serem detectados? Quanto mais estreitamente for possível definir a atividade alvo, melhor se pode adaptar um detector às suas especificidades e reduzir o potencial de classificações erradas”, [Sommer e Paxson, 2010].

Considerações Finais

Desde o momento em que as informações passaram a ser produzidas, transportadas e armazenadas em dispositivos tecnológicos surgiu a preocupação com a segurança, não só dos aparelhos, mas das informações contidas neles. É imprescindível para uma empresa o investimento em segurança da informação. Qualquer organização que utiliza da tecnologia como parte considerável do seu negócio necessita ter uma base confiável de segurança.

Investir em segurança da informação não garante que as informações estão salvas de qualquer ataque ou eventualidade, mas diminui drasticamente as chances de isso acontecer. Uma boa gestão de segurança ainda é prevenida caso algum problema venha a acontecer, com planos de ações para esses eventos.

Cada vez mais a SI se insere no dia-a-dia de pessoas ao redor do mundo como algo indispensável e que merece atenção. E em um ano como 2020, onde o trabalho remoto e aulas online se tornaram obrigatórios, a segurança da informação foi necessária como nunca, garantindo que a internet se tornasse um meio seguro para empresas, estudantes e demais usuários.

Segurança não se refere apenas a impedir riscos e sim tratá-los da melhor forma, com inteligência. Pode parecer difícil e caro para uma empresa a implementação de um sistema de segurança, mas nenhum esforço ou capital é demais, quando se trata de proteção para organização e seus bens. É importante definir bem os planos de segurança, visualizar os riscos e criar métodos de prevenção e ação.

REFERÊNCIAS

Relatório de ataques no primeiro semestre de 2020 no Brasil. Disponível em https://www.fortinetthreatinsiderlat.com/pt/Q2-2020/BR/html/trends#trends_position, acesso em 23 de Setembro de 2020.

LEMES, Leonardo. Redação "Trabalho remoto e a segurança da informação ", disponível em https://olhardigital.com.br/fique_seguro/colunistas/leonardo-lemes/post/trabalho_remoto_e_a_seguranca_da_informacao/87302, acesso em 28 de Setembro de 2020.

Instrução Normativa GSI/PR no 1, de 13 de junho de 2008. Disponível em http://dsic.planalto.gov.br/legislacao/in_01_gsidsic.pdf, acesso em 02 de Outubro de 2020.

PINHEIRO, Lena Viana Ribeiro e FERREZ, Helena Dodd. Tesauro Brasileiro de Ciência da informação. Disponível em https://ibict.br/images/internas/TESAURO-COMPLETO-FINAL-COM-CAPA-_24102014.pdf, acesso em 03 de Outubro de 2020.

Normas ISO/IEC da família 27000. Disponível em https://www.iso.org/home.html e https://www.portalgsti.com.br/2013/12/as-normas-da-familia-iso-27000.html, acesso em 03 de Outubro de 2020.

Carta de serviços do Instituto Nacional de Tecnologia da Informação (ITI). Disponível em https://www.gov.br/pt-br/orgaos/instituto-nacional-de-tecnologia-da-informacao, acesso em 03 de Outubro de 2020

Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção dos Dados. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm, acesso em 03 de Outubro de 2020.

Lei nº 13.853, de 8 de Julho de 2019, altera a Lei Geral de Proteção dos Dados e cria a Autoridade Nacional de Proteção de Dados. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1, acesso em 003 de Outubro de 2020.

Matéria do Wall Street Journal “Fraudadores usam IA para imitar voz de CEO em caso incomum de crime cibernético”. Disponível em https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402, acesso em 04 de Outubro de 2020.

Vianna, Eduardo Wallier. “Segurança da informação digital: proposta de modelo para a ciber proteção nacional”, 2019.

Rogalsky, Caroline. *Implantação de um sistema de gestão de segurança da informação: estudo de necessidade, criação e avaliação de um produto de informação (2005)*. Disponível em https://acervodigital.ufpr.br/handle/1884/48316, acesso em 19 de outubro de 2020.

Pessoa, Raimundo Alan Matos. *Um estudo de caso sobre a gestão da segurança da informação em uma instituição financeira (2012)*. Disponível em http://www2.uesb.br/computacao/wp-content/uploads/2014/09/UM-ESTUDO-DE-CASO-SOBRE-A-GEST%C3%83O-DA-SEGURAN%C3%87A-DA-INFORMA%C3%87%C3%83O-EM-UMA-INSTITUI%C3%87%C3%83O-FINANCEIRA.pdf, acesso em 18 de outubro de 2020.

Abreu, Leandro Farias dos Santos. *A Segurança da Informação nas Redes Sociais (2011)*. Disponível em http://www.fatecsp.br/dti/tcc/tcc0023.pdf, acesso em 19 de outubro de 2020.

Marciano, João Luiz e Lima-Marques, Mamede. *O enfoque social da segurança da informação (2011)*. Disponível em https://www.scielo.br/scielo.php?pid=S0100-19652006000300009&script=sci_abstract&tlng=pt, acesso em 18 de outubro de 2020.

Zanella, Tatiele. *Estudo sobre a quebra de confidencialidade da informação e mecanismos de segurança (2017)*. Disponível em https://repositorio.ucs.br/xmlui/handle/11338/3807, acesso em 19 de outubro de 2020.

Eiras, Marcelo Coradassi. *Engenharia Social e Estelionato Eletrônico (2004)*. Disponível em https://docplayer.com.br/983029-Engenharia-social-e-estelionato-eletronico.html, acesso em 20 de outubro de 2020.

Aramuni, João Paulo Carneiro e Maia, Luiz Cláudio. O impacto da engenharia social na Segurança da Informação: uma abordagem corporativa. Disponível em https://revistas.ufpr.br/atoz/article/view/64640, acesso em Outubro de 2020.

Hintzbergen, Jule e Kees; Smulders, André; Bars, Hans. *Fundamentos de segurança da informação: com base na ISO 27001 e ISO 27002 (2018).*

ABNT NBR ISO/IEC 27002. Disponível em https://jkolb.com.br/wp-content/uploads/2016/09/ABNT-NBRISOIEC27001-20060331Ed1.pdf, acesso em Dezembro de 2020.

ABNT NBR ISO/IEC 27002. Disponível em http://www.fieb.org.br/download/senai/nbr_iso_27002.pdf, acesso em Dezembro de 2020.

Principais tipos de ataques de sequestro de dado. Disponível em https://www.alertasecurity.com.br/conheca-os-principais-tipos-de-ataques-de-sequestro-de-dados/, acesso em Outubro de 2019.

Spywares. Disponível em https://www.welivesecurity.com/br/2019/10/17/spyware-brasil-esta-entre-os-paises-mais-afetados-por-essa-ameaca-silenciosa/, acesso em novembro de 2020.

[1]Fung, Carol J. and McCormick, Bill. (2015). Vguard: A distributed denial of service attack mitigation method using network function virtualization. In 2015 11th International Conference on Network and Service Management (CNSM). Disponível em http://dl.ifip.org/db/conf/cnsm/cnsm2015/1570165241.pdf. Acesso em Outubro de 2019.

Brasileiros criam software malicioso que se apresenta como uma atualização do Adobe Flash Player. Disponível em https://www.kaspersky.com.br/blog/primeiro-ransomware-brasileiro/5877/, acesso em outubro de 2019.

FBI emite alerta sobre ransomware MSIL/Samas. Disponível em https://canaltech.com.br/seguranca/fbi-emite-alerta-sobre-ransomware-capaz-de-infectar-backups-na-rede-61239/, acesso em outubro de 2019.

FBI alerta hospitais para possíveis ataques de ransomware. Disponível em https://olhardigital.com.br/noticia/fbi-alerta-hospitais-para-ameaca-crescente-e-iminente-de-ransomware/109501, acesso em novembro de 2020.

Primeiro ataque ransomware para Mac detectado. Disponível em https://www.bitmag.com.br/2016/03/primeiro-ataque-de-ransomware-para-mac-detectado-em-cliente-para-bittorrent/, acesso em outubro de 2019.

Backdoor. Disponível em https://www.psafe.com/blog/backdoor/, acesso em outubro de 2019.

Kumar, Sumeet e Carley, Kathleen. (2016). Understanding DDoS cyber-attacks using social media analytics. 231-236. 10.1109/ISI.2016.7745480. Disponível em https://www.researchgate.net/publication/310500648_Understanding_DDoS_cyber-attacks_using_social_media_analytics, acesso em outubro de 2019

Ataques Dos e DDoS. Disponível em https://www.infowester.com/ddos.php, acesso em outubro de 2019.

[2]StarHub (2016). Starhub confirma a causa de incidentes de banda larga em 22 e 24 de outubro de 2016. Disponível em http://bit.ly/2i8Uef0. Acesso em Outubro de 2019

Santos, Luiz Arthur Feitosa dos. (2011). Segurança da informação. Disponível em https://www.slideshare.net/luiz_arthur/seguranca-da-informao-introduo, acesso em 18 de Outubro de 2020.

Aramuni, João Paulo Carneiro, e Maia, Luiz Cláudio. O impacto da engenharia social na segurança da informação: uma abordagem orientada à gestão corporativa. Disponível em https://www.researchgate.net/publication/338560630_O_impacto_da_Engenharia_Social_na_Seguranca_da_Informacao_uma_abordagem_orientada_a_Gestao_Corporativa, acesso em 18 de Outubro de 2020.

ESET Security Report 2020. Disponivel em https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Security_Report_2020_BR-1.pdf, acesso em 18 de outubro de 2020.

O número crescente de violações de dados em hotéis. Disponível em https://www.hotelnewsnow.com/Articles/50937/Timeline-The-growing-number-of-hotel-data-breaches, acesso em 15 de novembro de 2020.

National Institute of Standards and Technology. Disponível em https://www.nist.gov, acesso em 15 de novembro de 2020.

Wueest, Candid. Teste em sites de hotéis. Disponível em https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/hotel-websites-leak-guest-data?es_p=9087455, acesso em 15 de novembro de 2020.

ESET Security Report 2020. Disponível em https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Security_Report_2020_BR-1.pdf, acesso em 15 de novembro de 2020.

Brasil é o país mais afetado por trojans bancários. Disponível em https://canaltech.com.br/seguranca/brasil-e-o-pais-mais-afetado-por-trojans-bancarios-diz-eset-138219/, acesso em 16 de novembro de 2020.

Silva, Iury Pereira. *Engenharia social como ameaça ao setor bancário: uso do phishing para coletar informações dos correntistas e a necessidade de estratégias de segurança*. Disponível em http://www.repositorio.ufc.br/bitstream/riufc/49703/1/2019_tcc_ipsilva.pdf, acesso em 16 de novembro de 2020.

KASPERSKY. The Tetrade: Malware bancário brasileiro se torna global. Disponível em https://securelist.com/the-tetrade-brazilian-banking-malware/97779/, acesso em 16 de novembro de 2020.

AV-TEST https://www.av-test.org/en/statistics/malware/,

Papastergiou S, Mouratidis H, Kalogeraki EM. Cyber Security Incident Handling, Warning and Response System for the European Critical Information Infrastructures (CyberSANE), 2019. Disponível em https://research.brighton.ac.uk/en/publications/cyber-security-incident-handling-warning-and-response-system-for-, acesso em 07 de novembro de 2020.

al H. Sarker1,2 , A. S. M. Kayes , Shahriar Badsha , Hamed Alqahtani , Paul Watters and Alex Ng. Cybersecurity data science: an overview from machine learning perspective, 2020. Disponível em https://journalofbigdata.springeropen.com/articles/10.1186/s40537-020-00318-5, acesso em 07 de novembro de 2020.

Instituto Ponemon. The State of Endpoint Security Risk: it's skyrocketing. Disponível em https://ponemonsullivanreport.com, acesso em 08 de novembro de 2020.

Relatório interno da NSCAI para o Congresso (2019). Disponível em https://drive.google.com/file/d/153OrxnuGEjsUvlxWsFYauslwNeCEkvUb/view, acesso em 08 de novembro de 2020.

R. Sommer e V. Paxson. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection, *2010 IEEE Symposium on Security and Privacy* , Berkeley / Oakland, CA, 2010, pp. 305-316. Disponível em https://www.icsi.berkeley.edu/icsi/node/4511, acesso em 08 de novembro de 2020.

Choi, Y., Liu, P., Shang, Z. *et al.* Usando o aprendizado profundo para resolver os desafios da segurança do computador: uma pesquisa, (2020). Disponível em https://doi.org/10.1186/s42400-020-00055-5, acesso em 08 de novembro de 2020.