www.alomorfia.com.br, ISSN 2594-5637

A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO PARA AS ORGANIZAÇÕES

Eliane Vendramini de Oliveira
elianevendramini@gmail.com

Rodrigo Filgueiras
rodrigo_filgueiras_95@hotmail.com

RESUMO

Juntamente com as vantagens da tecnologia e do uso da internet, criminosos e oportunistas podem se apropriarem de informações confidenciais e da privacidade os usuários. Surgiu assim, a Segurança da informação que possui a finalidade de proteger determinado grupo de dados. Essas medidas de segurança podem ser aplicadas em todas as empresas que trabalham com dados, pois toda organização gera informações próprias e devem ser preservadas para sua seguridade. Assim, a informação tem importância estratégica, é impulsionada com a utilização de Tecnologia da Informação nos processos organizacionais e deve ter proteção adequada. O objetivo do trabalho é fazer uma análise sobre a segurança da informação nos dias atuais, além de demonstrar a sua importância para todas as pessoas jurídicas e civis.

Palavras-chaves: Segurança da informação; Políticas de Segurança; Proteção da Informação;

ABSTRACT

Along with the advantages of technology and the use of the internet, criminals and opportunists can appropriate users' confidential and privacy information. Thus emerged, the Information Security that has the purpose of protecting a certain group of data. These security measures can be applied in all companies that work with data, as every organization generates its own information and must be preserved for its security. Thus, information has strategic importance, is driven by the use of Information Technology in

www.alomorfia.com.br, ISSN 2594-5637

organizational processes and must have adequate protection. The objective of the work is to analyze information security today, in addition to demonstrating its importance for all legal and civil entities.

Keywords: Information security; Security policies; Information Protection;

1- INTRODUÇÃO

Nos tempos atuais, com o avanço da tecnologia, podemos nos conectar a tudo e a todos por meio de diversos meios de comunicação. Atualmente a internet é o meio mais acessado do planeta pela facilidade de comunicação e, com a avalanche da globalização, o intercâmbio entre os países é como se estivessem fisicamente próximos. Ao lado desse mecanismo saudável, existem criminosos e oportunistas que se aproveitam das lacunas deixadas pela tecnologia e acaba sendo criada uma imagem de falta de segurança da informação e da privacidade nesse ambiente com o planeta conectado pelas tecnologias de comunicação e de computação.

Seguindo esse raciocínio, foi necessária criar meios para que pudessem combater o lado negativo e suas informações pessoais e de empresa fossem seguras.

Levando para o âmbito corporativo, são válidos pontuar que as informações das grandes empresas têm sido utilizadas de forma estratégica para que as instituições cresçam e se destaquem entre concorrentes, onde necessitam estar asseguradas quanto aos seus dados, pois quem detém dados e informações possui poder. As empresas fazem uso da informação para realizar decisões, fazendo com que alcancem objetivos e melhorem seu desempenho no mercado.

A informação é um recurso essencial para toda e qualquer organização, onde independente do seu tamanho e do segmento de atuação. É com essa informação que processos organizacionais funcionam, a produção de conhecimento acontece e o compartilhamento desse conhecimento é realizado.

Assim, a informação tem importância estratégica, é impulsionada com a utilização de Tecnologia da Informação (TI) nos processos organizacionais e deve ter proteção adequada.

www.alomorfia.com.br, ISSN 2594-5637

Segundo o Dicionário Brasileiro da Língua Portuguesa Michaelis, a palavra Segurança, vem do verbo segurar com significado de tonar(-se) seguro, estável; apoiar ou agarrar para que não caia ou não se arruíne; firmar(-se), sustentar(-se), suster(-se).

Sendo assim, este é o objetivo dos gestores de uma empresa, sempre estarem firmes para que nada saia fora do previsto.

A Segurança da informação engloba ações e boas práticas onde a finalidade é proteção de determinado grupo de dados.

Essas medidas de segurança podem ser aplicadas em todas as empresas que trabalham com dados, pois toda organização gera informações próprias e devem ser preservadas para sua seguridade.

Cinco são os pilares que sustentam todas as medidas tomadas para garantir a proteção dos dados, sendo eles a confidencialidade, autenticidade, integridade, disponibilidade e irretratabilidade.

O objetivo do trabalho é fazer uma análise sobre a segurança da informação nos dias atuais e sua justificativa é a importância da segurança de dados para todas as pessoas jurídicas e civis.

2 - METODOLOGIA

O presente trabalho tem sua metodologia fundamentada na revisão bibliográfica e plataformas virtuais. E teve sua realização de pesquisa utilizando o Google Chrome em um Notebook i5 2430M. A pesquisa apresentada é de caráter qualitativo pois apresenta uma revisão e análise das técnicas de segurança, não tratando dados estatísticos.

3- DESENVOLVIMENTO

Silva, L.W. (2001) relata que no início da década de 70, nos Estados Unidos, as empresas trabalhavam com a rede Intranet, que era ligada por fios de rede entre os computadores. Com o passar do tempo e o avanço da tecnologia, identificou-se a necessidade em algo melhor e com maior abrangência de troca das informações. Assim

www.alomorfia.com.br, ISSN 2594-5637

iniciou o estudo para criação da Internet, vindo a se tornar comercial no ano de 1987, chegando ao Brasil no ano de 1988.

A descoberta da Internet fez com que os avanços científicos fossem capazes de atingir grande marcos, como melhores programas, sistemas e até a comunicação se tornou melhor. Apesar de ser criada para ser algo benéfico, algumas pessoas denominadas hackers ou atacantes, utilizam da rede para seu próprio benefício e muitas vezes prejudicando terceiros.

E é por isso que a segurança da informação se tornou necessária, onde atualmente existem leis que determinam os direitos e deveres de todos os que estão nessa enorme rede que engloba o mundo todo.

A) Segurança Da Informação

A segurança da informação aborda a proteção de dados e preserva valores de uma organização ou uma pessoa física.

Segundo Coelho, Araújo e Bezerra (2014), "A informação pode existir em diversos formatos: impressa, armazenada eletronicamente, falada, transmitida pelo correio convencional de voz ou eletrônico etc. Seja qual for o formato ou meio de armazenamento ou transmissão, recomenda-se que ela seja protegida adequadamente, sendo assim é de responsabilidade da segurança da informação protegê-la de vários tipos de ameaça."

A Informação pode ser violada de diversas formas, pelo próprio usuário e no ambiente na qual se encontra, por terceiros ou atacantes.

DANTAS (2011) cita que a segurança da informação deve garantir três requisitos fundamentais, sendo eles: confidencialidade, integridade e disponibilidade, requisitos estes, que devem ser mantidos, pois são os princípios da segurança da informação.

A conservação desses princípios, utilizadas nos sistemas de informações, conforme SILVA, CARVALHO e TORRES (2003), exigem medidas de segurança, que são utilizadas também para garantir a autenticidade e a irretratabilidade. Todas as medidas utilizadas, independente do objetivo, precisam ser colocadas em prática antes da efetivação dos riscos.

www.alomorfia.com.br, ISSN 2594-5637

B) Pilares Da Segurança Da Informação

1- Confidencialidade: Primeiro pilar da segurança da informação, pois garante que os dados estejam acessíveis a determinados usuários e protegidos contra pessoas não autorizadas. É um componente essencial da privacidade, que se aplica especialmente a dados pessoais, sensíveis, financeiros, psicográficos e outras informações sigilosas. (GAT INFOSEC, 2021)

2- Integridade: Preservação, precisão, consistência e confiabilidade dos dados durante todo o seu ciclo de vida. Para erguer esse pilar em uma empresa, é preciso implementar mecanismos de controle para evitar que as informações sejam alteradas ou deletadas por pessoas não autorizadas. Frequentemente, a integridade dos dados é afetada por erros humanos, políticas de segurança inadequadas, processos falhos e cyber ataques. (GAT INFOSEC, 2021)

3- Disponibilidade: Para que um sistema de informação seja útil, é fundamental que seus dados estejam disponíveis sempre que necessário e garanta acesso em tempo integral pelos usuários finais. (GAT INFOSEC, 2021)

4- Autenticidade: Valida a autorização do usuário para acessar, transmitir e receber determinadas informações. Seus mecanismos básicos são logins e senhas, mas também podem ser utilizados recursos como a autenticação biométrica, por exemplo. Esse pilar confirma a identidade dos usuários antes de liberar o acesso aos sistemas e recursos, garantindo que não se passem por terceiros. (GAT INFOSEC, 2021)

5- Irretratabilidade: Também chamado de "não repúdio", do inglês *non-repudiation*. Esse pilar garante que uma pessoa ou entidade não possa negar a autoria da informação fornecida, como no caso do uso de certificados digitais para transações online e assinatura de documentos eletrônicos. Na gestão da segurança da informação, isso significa ser capaz de provar o que foi feito, quem fez e quando fez em um sistema, impossibilitando a negação das ações dos usuários. (GAT INFOSEC, 2021)

Através desses pilares é possível evitar ataques e fraudes, pois eles garantem a proteção para o usuário com o servidor e vice e versa não enviando dados falsos e

www.alomorfia.com.br, ISSN 2594-5637

dificultando para o terceiro que de fora tenta ver ou invadir o seu servidor, esses pilares são construídos através de criptografia. (KASPERSKY, 2021)

C) Criptografia

A criptografia na segurança virtual é uma ferramenta que converte os dados que antes eram legíveis e agora são codificados, podendo ser apenas descodificados no destinatário onde iriam esses dados. É um elemento fundamental da segurança de dados.

É a forma mais simples e mais importante de garantir que as informações do sistema de um computador não sejam roubadas e lidas por alguém que deseja usá-las para fins maliciosos.

No momento que se envia um dado ou informação através do servidor para a rede (internet), ele passa por uma série de dispositivos ao redor do mundo, que denomina internet pública, e nesse percurso que os dados percorrem, é onde os hackers podem ter acesso aos dados.

A criptografia é o uso de um conjunto de valores matemáticos que se casam tanto no remetente quanto destinatário, fazendo com que a mensagem seja decriptografada, utilizado duas formas mais comuns: assimétrica e simétrica. (KASPERSKY, 2021)

1- **Chaves de criptografia simétrica:** também conhecidas como criptografia de chave privada. A chave usada para codificar é a mesma usada para decodificar, sendo a melhor opção para usuários individuais e sistemas fechados. Caso contrário, a chave deve ser enviada ao destinatário. Isso aumenta o risco de comprometimento se for interceptada por um terceiro, como um hacker. Esse método é mais rápido do que o método assimétrico. (KASPERSKY, 2021)

2- **Chaves de criptografia assimétrica:** esse tipo usa duas chaves diferentes, uma pública e uma privada, que são vinculadas matematicamente. Essencialmente, as chaves são apenas grandes números que foram emparelhados um ao outro, mas não são idênticos, daí o termo assimétrico. A chave privada é mantida em segredo pelo usuário, e a chave pública também é compartilhada entre destinatários autorizados ou disponibilizada ao público em geral. (KASPERSKY, 2021)

www.alomorfia.com.br, ISSN 2594-5637

D) Firewall

Ao contrário da criptografia, o Firewall também conhecido na tradução do inglês, *Parede de fogo,* é aquela defesa que fica no servidor, impedindo que um hacker invada o próprio sistema, diferente da criptografiaonde o ataque acontece no momento da transmissão da mensagem na rede.

Segundo Jonathan Machado (2012),*"Aplicações com a função de firewall já são parte integrante de qualquer sistema operacional moderno, garantindo a segurança do computador desde o momento em que ele é ligado pela primeira vez. Os firewalls trabalham usando regras de segurança, fazendo com que pacotes de dados que estejam dentro das regras sejam aprovados, enquanto todos os outros nunca chegam ao destino final*."

E) Sistemas Operacionais: Linux E Windows

Os ataques em ambos os sistemas operacionais ocorrem diariamente e a todo o tempo, sabe-se que a maior parte das pessoas utilizam o sistema operacional Windows, no entanto os ataques a servidores Linux vêm aumentando cada vez mais, uma vez que ele tem seus códigos aberto a qualquer pessoa e além de ser um sistema operacional gratuito.

De acordo com a Kaspersky, esses invasores estão diversificando cada vez mais seus arsenais para conter ferramentas Linux, dando-lhes um alcance mais amplo sobre os sistemas que podem visar. "A tendência de aprimorar os conjuntos de ferramentas APT foi identificada por nossos especialistas muitas vezes no passado, e as ferramentas com foco em Linux não são exceção", disse Yury Namestnikov, Chefe da Equipe Global de Pesquisa e Análise da Kaspersky na Rússia.

Com o objetivo de proteger seus sistemas, os departamentos de TI e segurança estão usando Linux com mais frequência do que antes. Os agentes de ameaças estão respondendo a isso com a criação de ferramentas sofisticadas que são capazes de penetrar em tais sistemas.

F) Lei 13.709 (Lei Geral De Proteão De Dados)

www.alomorfia.com.br, ISSN 2594-5637

Com constantes ataques cibernéticos, a informações das empresas ficaram cada vez mais frágeis a perdas e danos recorrentes e não possuíam consequências legais, sendo assim, foi necessária a implementação na legislação brasileira.

Essas medidas conforme assegura a lei, são utilizadas justamente para evitar que dados sejam roubados por atacantes ou até mesmo vazados de má fé.

Em agosto de 2018, foi aprovada a Lei 13.709 (Lei Geral de Proteção de Dados) que adota medidas a serem adotadas em relação a proteção de dados.

Segundo Denis Zeferino (2020), " *A lei solicita que seja adotada uma forma diferente de trabalhar com dados, então, pontos como segurança, transparência e privacidade e proteção de dados pessoais se tornaram mais importantes. Agora, para as empresas que não respeitarem as diretrizes da lei, as multas podem chegar a valores de até R$50 milhões."*

4- RESULTADO

Ao utilizar a internet deve-se certificar de que os dados por meio dos pilares da segurança da informação deixam ainda mais seguros em relação ao uso da rede. Além de procurar sistemas operacionais que tenham melhor preparo para esse tipo de ataque, assinar um serviço de firewall é extremamente importante para aqueles que usam a internet como ferramenta do dia a dia como pagar contas e consultar serviços bancários.

5- CONCLUSÃO

O artigo apresenta como a informação é enviada de um servidor para o outro e as formas com quem elas podem ser interpretadas tanto aos olhos humanos quando aos olhos computacionais, que através de criptografia proporciona maiores garantias e segurança para navegar com tranquilidade prevenindo-se dos usuários mal-intencionados.

Essas orientações servem para observar e prevenir de modo geral toda a informação, pois até mesmos pessoas comuns são alvos de ataques, já as empresas de pequeno até grande porte se tornaram alvo frequente.

www.alomorfia.com.br, ISSN 2594-5637

6- REFERENCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO/IEC 17799:2001: Tecnologia da Informação - Código de prática para gestão da segurança da informação. Ri de Janeiro, 2001.

COELHO, Flávia Estélia Silva; ARAÚJO, Luiz Geraldo Segadas; BEZERRA, Edson Kowask. Gestão da Segurança da Informação NBR 27001 e NBR 27002. Rio de Janeiro-RJ: RNP/ESR, 2014

DANTAS, L.M. Segurança da Informação - Uma Abordagem Focada em gestão de Riscos. Olinda. Livro Rápido, 2011

Da redação. Hackers focam em ataques a servidores e estações de trabalho Linux. Cio From IDG. 14/09/2020. Disponível em: 7- https://www.tecmundo.com.br/firewall/182-o-que-e-firewall-.htm

GAT Infosec. Como fortalecer os 5 pilares da segurança da informação nas empresas. Disponível em: https://www.gat.digital/blog/5-pilares-da-seguranca-da-informacao/

Kaspersky. O que é criptografia de dados? Definição e explicação. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/encryption

Lei no 13.709, de 14 de agosto de 2018. Lei geral de Proteção de Dados pessoais (LGPD) Planalto da Republica. Disponível em: https://planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/l13709.htm

MACHADO, Jonathan. O que é firewall? Tecnomundo. 21/06/2012 ,Disponível em: https://www.tecmundo.com.br/firewall/182-o-que-e-firewall-.htm

Politize, 13/10/2017. O que é globalização?, 2017, Disponível em: https://www.politize.com.br/globalizacao-o-que-e/

Segurança, Michaelis UOL. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/seguranca/

Silva, LW.12/08/2001. Internet foi criada em 1969 com o nome ‘’Arpanet’’ nos EUA. Cotidiano – Folha de S.Paulo. Disponível em: https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml

www.alomorfia.com.br, ISSN 2594-5637

SILVA T.P; CARVALHO H; TORRES B.C. Segurança dos Sistemas de Informação - Gestão Estratégica da Segurança Empresarial. Portugal. Atlântico, 2003

ZEFERINO, Denis. O que é Segurança da Informação e qual sua importância? Certifiquei. Publicado em 27/07/2020. Disponível em: https://www.certifiquei.com.br/seguranca-informacao/