UNIVERSIDADE FEDERAL FLUMINENSE

JHONATAN ESTERQUE ALMEIDA

TÍTULO: VALOR DA SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS

NITERÓI

2022

JHONATAN ESTERQUE ALMEIDA

VALOR DA SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS

Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

Este trabalho foi defendido e aprovado pela banca em 01/112/2022

BANCA EXAMINADORA

Prof. Ricardo de Oliveira Nolasco, MSc. – Avaliador
UFF - Universidade Federal Fluminense

MARCOS FIALHO DE CARVALHO:66560543749

Assinado de forma digital por MARCOS FIALHO DE CARVALHO:66560543749
Dados: 2022.12.19 11:37:10 -03'00'

Marcos Fialho de Carvalho, MSc. Avaliador
UFRJ - Universidade Federal do Rio de Janeiro

Ficha catalográfica automática - SDC/BEE
Gerada com informações fornecidas pelo autor

A447v Almeida, JHONATAN ESTERQUE
VALOR DA SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS / JHONATAN ESTERQUE Almeida. - 2022.
29 f.

Orientador: RICARDO NOLASCO.
Coorientador: LEANDRO SOARES DE SOUZA.
Trabalho de Conclusão de Curso (graduação)-Universidade Federal Fluminense, Instituto de Computação, Niterói, 2022.

1. GESTÃO DA INFORMAÇÃO. 2. SEGURANÇA DA INFORMAÇÃO. 3. Produção intelectual. I. NOLASCO, RICARDO, orientador. II. SOUZA, LEANDRO SOARES DE, coorientador. III. Universidade Federal Fluminense. Instituto de Computação. IV. Título.

CDD - XXX

Bibliotecário responsável: Debora do Nascimento - CRB7/6368

JHONATAN ESTERQUE ALMEIDA

TÍTULO: VALOR DA SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS

Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

Este trabalho foi defendido e aprovado pela banca em DD/MM/AAAA.

BANCA EXAMINADORA

_____

Prof.ª Dr.ª Nome – Orientadora

UFF - Universidade Federal Fluminense

_____

Prof. Ms. Nome – Avaliador

URFJ – Universidade Federal do Rio de Janeiro

_____

Prof. Dr. Nome – Avaliador

UFF - Universidade Federal Fluminense

Dedico este trabalho a minha família.

AGRADECIMENTOS

Agradeço a Deus por essa oportunidade de estar concluindo essa etapa na minha vida.

Agradeço minha família, Jessicka, Sarah e Kaleb que foram minha maior motivação para não desistir.

Agradeço ao Orientador Ricardo Nolasco e o Coorientador Leandro Soares de Souza pelo direcionamento em minhas dúvidas.

Quem olha para fora sonha, quem olha para dentro desperta.

(Carl Jung)

RESUMO

Este estudo buscou de forma simples e objetiva mostrar o valor da segurança da informação nas empresas, sua origem, aspectos históricos, suas definições e quais são as consequências da falta dela, principalmente hoje, na era digital, onde um dos bens mais preciosos é a informação. Isso através de coletas de dados com base em pesquisa bibliográfica e exemplos de grandes empresas líderes de mercado que já sofreram as consequências da falta de segurança da informação, provando dessa forma que, ela é sim essencial para as empresas obterem sucesso. A política de segurança da informação é o principal elemento definidor das ações necessárias para a proteção das informações dentro de uma empresa, sendo inspirada nos padrões internacionais de melhores práticas de segurança da informação. Considerando a importância de medidas a serem tomadas como instrumento estratégico dentro das empresas, o estudo buscou discutir a segurança da informação.

Palavras-chave: Segurança; Informação; Empresas; Gestão.

ABSTRACT

This study sought, in a simple and objective way, to show the value of information security in companies, its origin, historical aspects, its configurations and what are the consequences of the lack of it, especially today, in the digital age, where one of the most precious assets is the information. This is done through data collection based on bibliographical research and examples of large market leading companies that already protect the consequences of lack of information security, thus proving that it is indeed essential for companies to succeed. The information security policy is the main defining element of the actions necessary for the protection of information within a company, being inspired by international standards of best practices in information security. Considering the importance of measures to be taken as a strategic instrument within companies, the study sought to discuss information security.

Keywords: Safety; Information; Companies; Management.

LISTA DE SIGLAS

ALPDP	Anteprojeto da Lei de Proteção de Dados Pessoais
ANPD	Autoridade Nacional de Proteção de Dados
IDS	Sistema de Detecção de Intrusão
IoT	Internet das Coisas
LGPD	Lei Geral de Proteção de Dados Pessoais
PCs	Computadores
RGPD	Regulamento Geral da Proteção de Dados
SI	Segurança da Informação
TI	Tecnologia da Informação

SUMÁRIO

1. INTRODUÇÃO

Este estudo objetiva discutir a Segurança da Informação (SI), frente a necessidade de proteção de dados na internet.

A segurança de dados, também conhecida como segurança da informação é um aspecto essencial da Tecnologia da Informação (TI) em organizações de qualquer tamanho e tipo. Este é um aspecto que tem a ver com a proteção dos dados contra acessos não autorizados e para protegê-los de possíveis corrupções ao longo de seu ciclo de vida.

A segurança de dados inclui conceitos como criptografia de dados, tokenização e práticas de gerenciamento de chaves que ajudam a proteger os dados em todos os aplicativos e plataformas de uma organização.

Atualmente, organizações em todo o mundo investem fortemente em tecnologia da informação relacionada à defesa cibernética para proteger seus ativos críticos: sua marca, capital intelectual e informações de clientes.

Em todas as questões de segurança de dados existem elementos comuns que todas as organizações devem levar em consideração ao aplicar suas medidas: pessoas, processos e tecnologia.

A segurança dos dados é uma questão muito importante que afeta quase todos nós. Existem cada vez mais produtos tecnológicos que de uma forma ou de outra devem ser levados em consideração por questões de segurança e que estão sendo introduzidos em nossas vidas diárias, de smartwatches a veículos autônomos. A era da Internet das Coisas (IoT) chegou e, claro, os *hackers* relacionados à IoT. Todos esses dispositivos conectados criam novas “conversas” entre dispositivos, interfaces, infraestruturas privadas e a nuvem, o que, por sua vez, produz mais oportunidades para os *hackers* espionarem. Tudo isso alimentou a demanda por soluções de segurança de dados e especialistas capazes de construir redes mais fortes e menos vulneráveis.

Tendências recentes mostraram que os ataques de *ransomware* estão aumentando em frequência e gravidade. Tornou-se um negócio em expansão para ladrões cibernéticos e *hackers*, que acessam a rede e sequestram dados e sistemas. Nos últimos meses, grandes empresas e outras organizações, bem como usuários

individuais, foram vítimas desses tipos de ataques e tiveram que pagar o resgate ou correr o risco de perder dados importante.

Pensar em segurança de dados e construir defesas desde o início é de vital importância. Os engenheiros de segurança visam proteger a rede contra ameaças desde o início até que sejam confiáveis e seguras. Os engenheiros de segurança projetam sistemas que protegem as coisas certas da maneira certa. Se o objetivo de um engenheiro de *software* é garantir que as coisas aconteçam, o objetivo de um engenheiro de segurança é garantir que coisas (ruins) não aconteçam, projetando, implementando e testando sistemas completos e seguros. A engenharia de segurança cobre muito terreno e inclui muitas medidas, desde testes regulares de segurança e revisões de código até a criação de arquiteturas de segurança e modelos de ameaças para manter uma rede bloqueada e segura de um ponto de vista holístico.

Se a engenharia de segurança de dados protege a rede e outros ativos físicos como servidores, computadores e bancos de dados, a criptografia protege os dados e arquivos reais armazenados neles ou trafegando entre eles pela Internet. As estratégias de criptografia são cruciais para qualquer empresa que usa a nuvem e são uma ótima maneira de proteger discos rígidos, dados e arquivos em trânsito por e-mail, em navegadores ou a caminho da nuvem.

No caso de os dados serem interceptados, a criptografia dificulta que os *hackers* façam qualquer coisa com eles. Isso ocorre porque os dados criptografados são ilegíveis por usuários não autorizados sem a chave de criptografia. A criptografia não deve ser deixada para o último e deve ser cuidadosamente integrada à rede e fluxo de trabalho existentes para ser mais bem-sucedida.

2. REVISÃO TEÓRICA

A internet é uma rede de conexões globais que permite o compartilhamento instantâneo de dados entre dispositivos. Ela foi criada a partir de pesquisas militares no auge da Guerra Fria, nos Estados Unidos. Definida inicialmente como Arpanet, tinha como intuito de realizar a comunicação do exército durante a guerra caso os meios de comunicação tradicionais da época fossem destruídos em ataques.

Segundo Kolbe Junior (2017) a informação tem atualmente um papel crucial para toda a sociedade, e também para as empresas.

A informação é um bem muito valioso, e nos dias atuais com o avanço e a multiplicação da tecnologia, mais do que nunca se faz necessário o controle adequado a esse conjunto de dados lógicos e materiais financeiros que compõem um sistema de informação. (KOLBE JUNIOR, 2017)

A política de segurança da informação tem muita importância no mundo de hoje, porque mesmo as empresas que ainda não dispõem de uma política de segurança, em determinado momento reconhecem a necessidade de implantá-la, considerando esta uma ferramenta essencial na segurança de uma organização.

Sêmola (2003, p. 12) define segurança da informação como "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade."

As organizações, independentemente de tamanho, pequena, média ou grande, buscam através de ferramentas e ações, executar práticas seguras para garantir a integridade de suas atividades e situação econômica. Tendo em vista essa preocupação, as organizações estão buscando a adoção de normas e práticas derivadas de padrões internacionais.

Dentro das organizações dos mais variados ramos, desde redes varejistas a redes de distribuição, o uso de tecnologias como: celulares, computadores, rádios, redes sem fio, entre outros, tornam possível a ocorrência de problemas de segurança diariamente. Sejam eles problemas decorrentes de invasão ou até mesmo, resultantes da comunicação entre pessoas. A definição de procedimentos, destinados a nortear condutas de como agir e, portar-se com relação ao sistema interno da empresa, uso de senhas, e acesso a informações privadas, entre outros, devem estar ao alcance dos usuários de sistema e sempre que possível, deverão ser descritos em

documentos que explanem a política de segurança da informação dentro da própria organização como forma de garantir a clareza e o uso dos princípios e das diretrizes utilizadas na empresa. Nesse sentido, é importante que as principais normas de segurança da informação sejam apresentadas para minimizar os riscos que as organizações sofrem na falta de conhecimentos destas. (KOLBE JUNIOR, 2017)

A segurança da informação é um dos assuntos de maior preocupação para as organizações em todo o mundo. Os responsáveis pelas áreas de sistemas estão sempre buscando ficar um passo à frente, tomando as devidas precauções para evitar ataques ou desastres nos dados da organização. No entanto, muitas vezes esses esforços não são roteados corretamente. (KOLBE JUNIOR, 2017)

A segurança da informação passou por uma evolução contínua durante a última década, de uma abordagem puramente tecnológica, onde as necessidades são atendidas pela aquisição de ferramentas para mitigar as mais recentes vulnerabilidades conhecidas, até uma abordagem dominada pela necessidade de justificar o investimento em segurança da informação como um bem essencial. Essa abordagem é baseada em uma gestão na qual os riscos são utilizados com base na otimização de índices de negócios, como custo / benefício.

O que sempre deve ser levado em consideração é que o problema de segurança é algo dinâmico, ou seja, não termina, na verdade é um erro acreditar que depois de ter uma solução de segurança a proteção máxima foi alcançada para sempre. A pior coisa que pode acontecer é que uma organização acredite estar protegida porque possui um antivírus, um *firewall* ou qualquer outro sistema de segurança ou qualquer tecnologia que possa existir e com isso acredita que é seguro. (KOLBE JUNIOR, 2017)

A maioria dos especialistas ressaltam que a segurança não é alcançada apenas com *hardware* e *software*, mas com uma estratégia abrangente que envolve políticas e práticas. Tais políticas levam à definição de papéis dentro da organização. O problema de segurança deve ser pensado e considerado desde o início de qualquer projeto e implementação. (KOLBE JUNIOR, 2017)

Outra ideia que deve ser levada em consideração, é que não há solução de segurança aplicável à todas as organizações. Em outras palavras, a solução que deve ser implementada em uma universidade é diferente daquela que seria aplicada a um

banco; e a estratégia para proteger uma empresa privada também é diferente daquela para fornecer proteção às informações da polícia ou das forças armadas.

Embora muitas pessoas associem a ideia de proteção do computador a *hackers*, essa é apenas uma das ameaças a serem consideradas ao projetar um sistema de segurança. A segurança do computador ou a segurança da informação têm muitas frentes. A tecnologia é apenas um aspecto da segurança. A segurança é um monstro que tem muitos tentáculos ou arestas que devem ser levados em consideração. (KOLBE JUNIOR, 2017)

Do ponto de vista dos elementos técnicos, existem várias camadas de segurança que permitem garantir a segurança do perímetro, *gateways* de segurança da *Web*, correio, criptografia, inspeção de dados, incluindo sistemas de arquivamento, *backup* de dados, gerenciamento de identidades, identificação de vulnerabilidades para proteção de *endpoint* com serviços possuindo antivírus, *firewalls*, registros de codificadores, sistemas de *backups* de arquivos, controle de periféricos e controle do vazamento de informações entre alguns elementos a serem considerados.

Uma das frentes de segurança é a proteção física de computadores, por exemplo, a proteção de servidores em uma sala especialmente condicionada. Nesta área, podem ser incluídas soluções de controle de acesso para restringir a entrada de pessoas não autorizadas na área de equipamentos de informática. Entre as soluções de controle podemos citar, dispositivos biométricos que realizam leitura de impressões digitais, dispositivos que reconhecem a palma da mão ou íris do olho.

Outro ponto importante a ser observado é que você pode ter a melhor infraestrutura de rede, mas se a porta do centro de computadores estiver aberta, ela não funcionará. Para segurança física, é necessário adicionar sistemas de controle de incêndio, segurança elétrica, sistemas UPS, geradores elétricos, entre outros. (KOLBE JUNIOR, 2017)

Os ataques a uma organização não só podem vir de fora, mas também de dentro. É por isso que, de acordo com os principais estudos de segurança, salienta-se que 70% do desvio de informações privilegiadas vem da organização. Muitas vezes, os responsáveis pelos sistemas se preocupam com *hackers*, mas são os próprios funcionários que podem manipular indevidamente as informações.

Muitas organizações estão prestando atenção especial à identificação daqueles que têm acesso à informação. Concentrando-se principalmente em perfis de usuário, estabelecendo quem tem acesso a determinados departamentos e quem precisa mostrar identificação para acessar determinadas áreas. As políticas de segurança devem ser aplicadas a toda a organização, para isso devemos estabelecer uma análise de risco.

No campo da avaliação de riscos em segurança integral, implica afastar-se de elementos de subjetividade e nos concentrar em abordagens estatísticas e de gerenciamento adequadas, o que nos obriga a criar estruturas objetivas para que possam ser auditadas e gerem soluções aos problemas estabelecidos na análise. (KOLBE JUNIOR, 2017)

Em uma rede interna, o acesso é mais aberto, portanto, é mais fácil atacar um servidor, razão pela qual uma solução para esse tipo de ataque é tratar a rede interna como se fosse a Internet. Sob esse esquema, os *firewalls* e o Sistema de Detecção de Intrusão (IDS) devem ser instalados, além de separar os diferentes ambientes de uma organização: desenvolvimento, teste, produção, etc. e tratar cada ambiente como uma rede separada, conectada aos demais por meio de um *firewall* central. Dessa forma, se alguém conseguir quebrar a segurança, ele atacará apenas uma parte da rede ou apenas participará da informação.

É importante que as organizações se preocupem em revisar os antecedentes ao contratar funcionários. Visto que, ao contratar alguém como administrador do sistema essa pessoa terá acesso aos *backups* de informações, portanto, é necessário que seja alguém confiável, para que não se corra risco de informações confidenciais serem passadas à concorrência.

Outro componente de uma estratégia de segurança são as políticas. Segundo especialistas, uma empresa não deve negligenciar a questão da atribuição de função dentro da estratégia. Dependendo do nível de segurança que se pretende atingir, é possível implementar políticas relacionadas ao uso de *software* em computadores (PCs), como regulamentos para usar apenas o *software* autorizado pela área de sistemas. Você também pode ter políticas relacionadas a atualizações de antivírus e detecção de ataques.

Existem também mecanismos de segurança que tentam melhorar o problema de segurança de uma rede de um ponto de vista muito mais ativo. Os mecanismos de proteção de informações e os mecanismos tradicionais de prevenção e detecção são usados para proteger os recursos da rede, detectando deficiências de segurança e reagindo posteriormente para solucionar esses problemas. Como novidade, esses novos elementos alteram as regras do jogo, oferecendo a possibilidade de tomar a iniciativa usando técnicas de monitoramento para registrar e analisar as ações dos atacantes para aprender com seus conhecimentos. (KOLBE JUNIOR, 2017)

Por outro lado, os elementos de detecção que vimos tentam unir a capacidade de bloqueio dos mecanismos de prevenção às capacidades de análise dos sistemas de detecção. Conhecidos como sistemas de prevenção de intrusões, esses novos elementos são considerados a evolução lógica dos sistemas tradicionais de detecção de intrusos.

Finalmente, um caso de interesse especial para os sistemas de detecção são os ataques distribuídos. Esses ataques não podem ser detectados isoladamente, mas é necessário correlacionar várias pistas encontradas em computadores diferentes em uma rede. Duas das propostas mais usadas para criar sistemas capazes de detectar esses ataques são o uso de nós dedicados (através de uma arquitetura centralizada ou hierárquica) e o uso de nós distribuídos (através de uma arquitetura baseada em código móvel ou da cooperação de uma etapa da mensagem).

Além disso, parte de uma estratégia de segurança são os planos de recuperação de desastres. Os especialistas concordam que não apenas pessoas de sistemas devem estar envolvidas nessa tarefa, mas membros de todas as áreas da organização.

A busca pela segurança é imparável e a cada dia mais complexa tecnologicamente. Novos modos de ataque surgem continuamente. O importante é que as organizações fiquem atentas a possíveis ataques e utilizem tecnologias para proteger adequadamente suas informações. (KOLBE JUNIOR, 2017)

No Brasil, o instituto “privacidade” foi abordado de forma implícita na Constituição do Império, em 1824, ao se referir ao “Segredo da Carta” e a “Inviolabilidade da casa”, protegendo o meio físico e não o conteúdo presente.

> No entanto, naquele momento, a privacidade estava submetida a um conceito mais lastreado na propriedade, ou seja, a carta magna protegia o meio físico e não o conteúdo em si. Por isso, vê-se apenas referência ao sigilo da correspondência e à inviolabilidade do domicílio. Perceba-se que não há uma proteção da privacidade por si só, pelo seu conteúdo ou por um aspecto mais subjetivo. O que se protegia ali era a invasão, o ato de romper barreiras físicas. (MACIEL, 2019, p. 7).

O artigo 5º, inciso LXXII, da Constituição Federal, prevê o Habeas Data considerado um remédio constitucional designado para assegurar que o cidadão tenha direito e acesso aos dados e informações que estão sendo utilizados pelo governo ou por empresas privadas com caráter público, assim temos o direito de sabermos o que o Estado sabe e como usa os dados e informações sobre nós.

> LXXII - conceder-se-á habeas data:
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

Em 1990, com o Código de Defesa do Consumidor, começou a ter uma preocupação maior em relação ao Banco de Dados do Consumidor. O consumidor passou a ter direito de obter informações de seus cadastros e dados pessoais, MACIEL (2019) alega que, embora o Código citado não tenha previsto o consentimento para coletar tais dados, exigiu que o consumidor fosse informado sobre a abertura do cadastro.

Com a Lei de Interceptação Telefônica e Telemática, em 1996, regulamentou o direito a intimidade da pessoa investigada, que apenas mediante a ordem judicial poderia haver o rompimento de tal privacidade. O texto constitucional está plenamente vinculado com a proteção da intimidade, com a proteção da privacidade, com a proteção da liberdade de expressão, por isso as demais pessoas não podem ser envolvidas e ter sua intimidade devassada só porque um determinado indivíduo das suas relações de amizade ou familiares está sendo investigado.

A inviolabilidade da vida privada como direito da personalidade, foi reconhecida em 2002, com o novo Código Civil. O conceito de privacidade estava voltado ao íntimo das pessoas, revelando a privacidade como um direito subjetivo e não focado no direito à propriedade.

Em 2011, começou a vigorar a Lei do Cadastro Positivo (Lei nº 12.414/11) disciplina a formação e consulta a bancos de dados com informações de

adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Com a aprovação da Lei Geral de Proteção de Dados, esta lei precisou de mudanças para se adequar e foi feita através da Lei Complementar nº 166 de 08 de Abril de 2019. Maciel fala sobre essa adequação:

> Assim, a partir da sua entrada em vigor, as pessoas físicas e jurídicas (cadastrados) serão inscritas automaticamente, sem necessidade de consentimento prévio, assegurando, todavia, o direito de exclusão e respeitado o princípio da finalidade. Interessante que para fornecer o histórico de crédito (conjunto de dados financeiros e de pagamentos, relativos às operações de crédito e obrigações de pagamento adimplidas ou em andamento por pessoa natural ou jurídica) do cadastrado para um consulente é preciso de autorização específica do cadastrado. (MACIEL, 2019, p. 11)

Ainda em 2011, a Lei de Acesso à Informação (LAI) (Lei nº 12.527/11), regulamenta o direito constitucional de acesso dos cidadãos às informações públicas e é aplicável aos três poderes da União, dos estados, do Distrito Federal e dos municípios, segundo Maciel (2019):

> [...] trouxe a definição de informação pessoal como sendo aquela relacionada à pessoa natural identificada ou identificável, determinando aos órgãos públicos e entidade do poder público a proteção da informação sigilosa e pessoal, observando a sua “disponibilidade, autenticidade, integridade e eventual restrição de acesso. (MACIEL, 2019, p. 11).

Em 2012, foi sancionada a Lei 12.737/12, a Lei Carolina Dieckmann, onde ocorreu uma alteração no Código Penal Brasileiro voltada para crimes virtuais e delitos da informática. Esse foi o primeiro texto que tipificou os crimes cibernéticos, tendo foco nas invasões a dispositivos que acontecem sem a permissão do proprietário. A Lei recebeu esse nome devido a atriz Carolina Dieckmann viver um episódio onde hackers invadiram seu computador e espalharam diversas fotos íntimas. Na época, o caso ganhou grande notoriedade.

Foi editado em 2013, o Decreto do Comércio eletrônico nº 7962/13 que Regulamenta a Lei nº 8.078/90, que visava atualizar uma parte do Código do Consumidor determinando ao lojista/fornecedor utilizar de meios para a proteção de dados do consumidor e do seu meio de pagamento.

De acordo com a Lei n. 13.709, de 14 de agosto de 2018:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direto público ou privado, com o objetivo de proteger os diretos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Pinheiro (2018), postula que a partir de 1990 a inspiração e o surgimento de regulamentação de proteção de dados pessoais têm total relação com o desenvolvimento do modelo de negócios da economia digital. Havendo esse compromisso das instituições com os indivíduos, cidadãos desta atual sociedade digital garantindo os direitos humanos fundamentais e sua proteção, como o da privacidade, já declarado desde a Declaração Universal dos Direitos Humanos de 1948.

Na União Europeia foi promulgada a Diretiva Europeia de Proteção de Dados Pessoais (95/96/EC), colocando os membros do bloco econômico sob a mesma legislação (PARLAMENTO EUROPEU; CONSELHO EUROPEU, 1995) que depois da sua substituição, em maio de 2018, influenciou a Lei Geral de Proteção de Dados Pessoais, Lei Nº 13.709, de 14 de agosto de 2018, conhecida como LGPD. (STELZER, J et al., 2019 apud BRASIL, 2019d). Assim contabilizando 12 países com as normas de proteção de dados, como por exemplo: Brasil, Argentina, Chile, Peru, Venezuela, etc.

A Lei Geral de Proteção de Dados Pessoais (LGPD) surge com o intuito de proteger os direitos humanos fundamentais, tais como a privacidade, honra, direito de imagem e dignidade. Com o desdobramento da globalização houve um grande aumento da necessidade das leis especificas para proteção de dados pessoais, trazendo a importância das informações. Dizendo assim que as informações passaram a ser um ativo de alta relevância para os governantes e empresários. (PINHEIRO, 2018).

Stelzer, J. et al. (2019), discorre que é de suma importância conceituar dado pessoal como informação relacionada à pessoa natural identificada ou identificável, podendo-se dizer que se trata de informação que, isolada ou associada, seja capaz de permitir a identificação de uma pessoa natural. Logo, nome, prenome, estado civil, número do Cadastro da Pessoa Física, número da cédula de identidade, são exemplos de dados pessoais, o que permite distinguir de dados gerais que não possuem vínculo objetivo com a pessoa. (STELZER, J et. al., 2019 apud DONEDA, 2006, p. 157).

Destaca-se dentro da LGPD as regras sobre os padrões de segurança:

Regras essas que são padrões de segurança da informação e medidas

> administrativas capazes de proteger os dados pessoais que deverão ser cumpridas pelos controladores e pelos operadores (aquele que realiza o tratamento de dados pessoais em nome do controlador). Ou seja, medidas técnicas adotadas no âmbito da tecnologia da informação e administrativas políticas corporativas, gestão estratégica e capacitação. (STELZER, J. et al, 2019 apud BRUNO, 2019, p. 330).

A LGPD foi promulgada pelo presidente Michel Temer no dia 14 de agosto de 2018 e foi originária do PLC Nº 53/2018. É uma legislação técnica, que reúne itens de controle para assegurar o cumprimento das garantias previstas e da proteção dos direitos humanos.

No cenário brasileiro, a LGPD se consolida em um importante momento na nossa legislação, que altera claramente o modelo atual de coleta e tratamento indiscriminado de dados pessoais, para adotar então o modelo onde somente será coletado aquilo que realmente é necessário. A LGPD traz consigo fundamentos que reforçam a proteção de direitos e garantias da pessoa natural, desde o respeito à privacidade, à autodeterminação informativa, à liberdade de expressão, à inviolabilidade da intimidade, ao desenvolvimento econômico e tecnológico, até a livre iniciativa e respeitos aos direitos humanos.

A LGPD abrange qualquer pessoa natural ou jurídica, de direito público ou privado, em meio físico ou digital, visando ou não à oferta ou ao fornecimento de bens e serviços, desde que seja em território nacional.

Como relembra Vainzof (2019, p.116), a LGPD abarca absolutamente todas as hipóteses de manuseio de dados, sendo assim, dados pessoais arquivados, mesmo que não sejam processados, estão em tratamento e precisarão ter uma base legal para permanecer sob a responsabilidade do agente de tratamento.

A LPGD complementa e unifica um conjunto de mais de quarenta normas setoriais que regulam, de forma direta e indireta, a proteção da privacidade e dos dados pessoais no Brasil. Ela também busca equilibrar interesses econômicos e sociais, garantindo a continuidade de decisões automatizadas e limitando abusos nesse processo, por meio da diminuição da discordância de informações, e por consequência, do poder entre o indivíduo, setor privado e o Estado (MONTEIRO, 2018).

As instituições que não estiverem em conformidade com a LGPD, podem vir a sofrer sanções na esfera administrativa, aplicada pela autoridade competente de proteção de dados, que pode ser desde uma simples advertência, ou até mesmo, uma

multa de até 2% do faturamento anual, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

Rocha, C. et al. (2019), postula que a nova lei de proteção de dados LGPD é de atual discussão e um novo paradigma da segurança de dados, principalmente nas empresas. A LGPD está forçando mudanças significativas nas empresas que lidam com dados on-line e off-line dos seus usuários, alterando a forma de proteção de dados brasileiros. É uma lei que estabelece regras bem definidas para coleta, uso, tratamento e armazenarmos dos dados pessoais, e afeta todos os setores da economia, inclusive a relação de clientes e fornecedores de produtos e serviços, empregado e empregador, relações comerciais nacionais e internacionais, e qualquer outro tipo de relação que envolvam coleta de dados pessoais, tanto no ambiente digital e fora do mesmo.

Para as empresas, que visam estrategicamente o compromisso de oferecer atividades de qualidade através da tecnologia da informação, é fundamental assegurar a proteção deste ativo. O meio aconselhado como mais assertivo é a implantação de um conjunto de normas e diretrizes que estabeleça a aplicação dos sistemas das organizações. (ROCHA, C et al., 2019).

Em linhas gerais, esse novo princípio faz com que as empresas analisem de fato os dados que fazem tratamento. A utilização desses dados requer das empresas a utilização consciente, inteligente e responsável. Todas as empresas que processam dados pessoais tiveram que adotar as medidas exigidas. Cabe às empresas e não somente apenas a administração pública, a responsabilidade de identificar os riscos e aplicar a medida necessária para mitigá-los. (MORAES, 2019).

Para atender essa nova legislação, as empresas, através dos seus agentes de tratamento, deverão manter registros das operações de dados pessoais e poderão ser exigidas da Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por zelar pela proteção dos dados pessoais e por fiscalizar o cumprimento da LGPD no Brasil, a produzirem relatórios de impacto à proteção de dados pessoais, incluindo a descrição dos tipos de dados coletados, além do motivo da coleta e a metodologia utilizada nessa coleta para proteção da segurança das informações. Tudo isso, de acordo com o artigo 38, da lei n 13.709, de 14 de agosto de 2018.

3. CONCLUSÃO

Um dos maiores problemas na Tecnologia da Informação encontra-se no fato de não existir apenas uma solução definida para tratar as ameaças e ataques à dados relacionados à segurança da informação. A conscientização e o treinamento de usuários de sistemas de informação são as principais ferramentas indispensáveis para combater a possíveis ataques ao sistema.

Apesar de parecer algo que não preocupa a sociedade, sua aparente simplicidade esconde uma perigosa forma de obter informações, e uma vez ignorada pode causar uma ameaça séria, essa forma de ataque jamais pode ser ignorada.

A dependência das organizações com relação a política de informação é inquestionável, já que os sistemas de informação se tornam cada vez mais vulneráveis a ameaça. Portanto, é preciso medidas que aumentem a segurança das empresas. Dentre as medidas de segurança a serem tomadas e implantadas então a norma NBR ISO 27002 que é a evolução da 17799. Esta norma trata da gestão de segurança da informação, e cobre os mais diversos tópicos da área de segurança, possuindo um grande número de controle e requerimentos que devem ser atendidos para garantir a segurança das informações dentro de uma empresa.

A implementação da segurança da informação em uma organização pode proteger a tecnologia e os ativos de informação que ela usa, prevenindo, detectando e respondendo a ameaças internas e externas. A alta administração e a TI são responsáveis pela estratégia de segurança da informação da organização.

Para apoiar a estratégia de segurança da informação, é essencial melhorar a conscientização da equipe sobre questões de segurança da informação por meio de treinamentos. As organizações também precisam impor suas políticas de segurança da informação e revisá-las regularmente para atender aos requisitos de segurança.

A Gestão de Segurança da Informação consiste em um componente estratégico ao negócio das organizações empresariais. Ainda que existam áreas que de forma aparente não fazem sentido ter a segurança da informação, o gestor de segurança deve ficar atento para propor práticas que estejam em conformidade com a norma escolhida.

Para finalizar deve-se salientar que o estudo não buscou determinar completamente os resultados, e esgotar a temática discutida. De forma contrária, buscou incentivar mais estudos sobre os temas discutidos.

4. REFERÊNCIAS BIBLIOGRÁFICAS

[1]. AGRELA, Lucas. **O escândalo de vazamento de dados do Facebook é muito pior do que parecia.** https://exame.abril.com.br/tecnologia/o-escandalo-de-vazamento-de-dados-do-facebook-e-muito-pior-do-que-parecia/.

[2]. ALBERTIN, A. L. **Administração de informática: funções e fatores críticos de sucesso.** São Paulo: Atlas, 2006.

[3]. ASSIS, CB. **Governança e gestão da tecnologia da informação**: diferenças na aplicação em empresas brasileiras I C.B. Assis. - São Paulo, 2011.

[4]. BAARS, Hans; HINTZBERGEN, Kees; HINTZBERGEN, Jule; SMULDERS, André. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.** São Paulo, 2018.

[5]. BASTO, Fabrício. **ITIL – A certificação do momento**. Disponível em; <http://analistati.com/itil-a-certificacao-do-momento/>.

[6]. CARLA PINTO, Ana. **Mecanismos para Gerência de Segurança em redes**. Porto Alegre: UFRGS, 2003.

[7]. CARVALHO, Pedro F. **Melhoria de serviço continuada**. Disponível em: <http://pt.scribd.com/doc/86768391/Itil-Melhoria-de-Servico-ada>.

[8]. CARVALHO, Tereza C. M. B. **Organização e Coordenação Arquiteturas de Redes Computadores OSI e TCP/IP.** São Paulo. Makron Books. 1994.

[9]. CASTRO, Jaime. **Sistema de Gestão de Segurança da Informação baseado na ISO 27001** e 27002. Wordpress, 2010.

[10]. CESTARI FILHO, Fellcio. **ITIL**: Information Technology Infrastructure Library. Rio de Janeiro: RNP/ESR, 2011.

[11]. CHIARI, Renê. **Principais diferenças entre a ITIL v2 e v3 – I**. Disponível em: <http://www.macdos.com.br/tag/itil/>.

[12]. COMER, Douglas. E. **Interligação em Rede com TCP/IP – Princípios, Protocolos e Arquitetura***.* Editora Campus, 1998.

[13]. DERFLER, Frank J. e JR. e FREED, Les. **Como funcionam as redes**. São Paulo. ZD Press. 1999.

[14]. DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação.** Rio de Janeiro: Axcel Books, 2000.

[15]. DOROW, Emerson. **ITIL e o ciclo de vida: Estratégia do Serviço**. Disponível em: <http://www.governancadeti.com/2010/10/itil-e-o-ciclo-de-vida-estrategia-do-servico/>.

[16]. EDDINGS, Joshua. **Como funciona a Internet.** Editora Quark, São Paulo, 1997.

[17]. FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a Governança de TI:** da Estratégia à Gestão dos Processos e Serviços. Rio de Janeiro, Brasport, 2016.

[18]. FOINA, Paulo Rogério. **Tecnologia de Informação: planejamento e gestão**. São Paulo: Atlas, 2011.

[19]. FONTES, Edison. **Políticas e normas para a segurança da informação.** Como desenvolver implantar e manter regulamentos para a proteção da informação nas organizações. Rio de Janeiro: Braspot, 2012.

[20]. GONZALEZ, R. S. **Governança e Sustentabilidade**. São Paulo, 07 maio 2009. Disponível em: <http://grcnews.blogspot.com/2009/05/governanca-e-sustentabilidade-por.html>.

[21]. INSTITUTO ONLINE. **Entendendo e implementando a norma ABNT NBR ISO/IEC 17799:2005:** aspectos teóricos e práticos para a implantação da norma ABNT ISO/IEC 17799:2005. Revisão 1.0. p. 1-84. Instituto OnLine, 2010.

[22]. ISO/IEC 17799, **Information Technology – code of practice for information security ITGI.** Management Guidelines to COBIT. 3.ed. IT Governance Institute, 2000a. management. International Organization of Standardization (ISO), Switzerland, 2005.

[23]. KERZNER, H. **Gestão de projetos: as melhoras práticas.** Porto Alegre: Bookman, 2002.

[24]. KOLBE, JUNIOR, Armando. **Sistemas de segurança da informação na era do conhecimento.** 2017.

[25]. KOTLER, P. **Administração e marketing. Análise, planejamento, implementação e controle.** 5ª ed. São Paulo. Editora Atlas, 1998.

[26]. LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Metodologia Científica**. São Paulo: Atlas, 2008.

[27]. LAUDON, J.P.; LAUDON, K.C. **Gerenciamento de sistemas de informação.** 5ª ed. São Paulo: Pearson, 2004.

[28]. LENNERT, Luiz: OLIVEIRA, Marcos. **O que é Engenharia Social.** Revista gestão de riscos**,** Ed.64,2011.

[29]. Lopes, Raquel; **Melhores Práticas para a Gerência de Redes de Computadores.** 1º ed. Editora Campus. 2003.

[30]. LYRA, Maurício. **Governança da Segurança da Informação**. Brasília, 2015.

[31]. MACÊDO, Diogo. **Introdução a ITIL**: conceitos básicos, história e organizações. Disponível em: <http://www.diegomacedo.com.br/introducao-a-itil-conceitos-basicos-historia-e-organizacoes/>. Acesso em janeiro de 2020.

[32]. MACHADO, C. P. **Responsabilidade social e governança. O debate e as implicações.** São Paulo: Thomson, 2006.

[33]. MARTINS, Gilberto de Andrade; LINTZ, Alexandre. **Guia para Elaboração de Monografias e Trabalhos de Conclusão de Curso**. São Paulo: Atlas, 2000.

[34]. MATIAS, A.B.: CENTRO DE PESQUISAS EM FINANÇAS. **Finanças Corporativas de longo prazo: criação de valor com sustentabilidade financeira**. São Paulo: Atlas, v. 2, 2007.

[35]. MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar:** ataques de hackers – controlando o fator humano na segurança da Informação. São Paulo: Makron, 2003.

[36]. MORAES, W.N. **Análise de investimentos em empresas de Internet: estudo de casos múltiplos usando o método do AHP – Analytic Hierarchy Process.** Dissertação (Mestrado). Departamento de Engenharia de Produção, Escola Politécnica, Universidade de São Paulo, São Paulo, 2003.

[37]. NUNES, Breno O. **ITIL V3**: Operação do serviço, metas e objetivos. Disponível em: <http://tiinteligente.blogspot.com.br/2011/12/itil-v3-operacao-do-servico-metas-e.html>. Acesso em janeiro de 2020.

[38]. O, BRIEN, J.A. **Sistemas de informação e as decisões gerenciais na era da Internet.** 2ª ed. São Paulo: Saraiva, 2004.

[39]. O GLOBO. **Facebook pagará multa recorde de US$ 5 bi para encerrar investigação sobre vazamento de dados.** https://extra.globo.com/noticias/economia/facebook-pagara-multa-recorde-de-us-5-bi-para-encerrar-investigacao-sobre-vazamento-de-dados-23828873.html

[40]. OLIVEIRA, Jayr Figueiredo. **Sistemas de Informação versus Tecnologias da Informação: um impasse empresarial**. São Paulo: Érica, 2014.

[41]. ÓRTICA, E. A.; CLEMENTI, S.; CARVALHO, T. C. M. B. Governança de TI: Comparativo entre COBIT e ITIL. In: **CONGRESSO ANUAL DE TECNOLOGIA DA INFORMAÇÃO**, 2004 São Paulo. Anais. São Paulo: FGV-EAESP, 2004.

[42]. PEREIRA, Cristiane. **Segurança em Intranet.** Brasília: UNB, 2003.

[43]. PRADO, Antonio F. **Aplicações Internet, Intranet e Extranet como diferencial competitivo nas organizações.** São Carlos: UFSCar, 2002.

[44]. PRESSMAN, Roger S. **Engenharia de Software**, Makron Books, 1995.

[45]. RAMOS, Anderson (Org.). **Security Officer - 1: Guia oficial para formação de gestores em Segurança da Informação**; Porto Alegre: Zouk, 2006. (Modulo Security Solutions) Revista FAE BUSINESS. n.3, set. 2002.

[46]. SAVIANI, J. R. **Analista de negócios e da informação: o perfil moderno de um profissional que utiliza a informática para alavancar os negócios empresariais.** São Paulo: Atlas, 2015.

[47]. SCHROEDER, Isley Roberto. **O Paradigma da Informática: gerar lucro para as empresas**. São Paulo: Nobel, 2002.

[48]. SECURATO, J.R. **Decisões financeiras em condição de risco**. 2. ed. São Paulo: Saint Paul Editora, 2007.

[49]. SHANG, David J.; MOON, Sylvia. **Segredos de Segurança em Rede.** Rio de Janeiro: Berkeley, 1994.

[50]. SOUSA, B. Lindeberg, **TCP/IP Básico Conectividade em Redes.** 3,ed.2006. CAMPOS, André L. N. **Sistema de segurança da informação:** controlando os riscos. Florianópolis: Visual Books, 2006.

[51]. UOL. **Banco Inter confirma vazamento de dados e culpa "pessoa autorizada".**https://www.uol.com.br/tilt/noticias/redacao/2018/08/17/banco-inter-confirma-vazamento-de-dados-apos-ataque-hacker.htm/.

[52]. VEJA. **Banco Inter vai pagar R$ 1,5 milhão por vazamento de dados de clientes**.https://veja.abril.com.br/economia/banco-inter-vai-pagar-r-15-milhao-por-vazamento-de-dados-de-clientes/

[53]. WEILL, Peter; ROSS, Jeanne. **Governança de Tecnologia da Informação**. São Paulo: M. Books, 2016.