

CENTRO UNIVERSITÁRIO BRASILEIRO – UNIBRA CURSO DE
GRADUAÇÃO TECNÓLOGO EM REDES DE COMPUTADORES

DIOGO SOUZA DELGADO

ERIKSON LUAN DA SILVA LIMA

IVANEIDE GONZAGA SALES

**O AVANÇO NA COLETA DE DADOS, SEU IMPACTO
PARA O MEIO TECNOLÓGICO E OS PROFISSIONAIS
DE SEGURANÇA DE REDES**

DIOGO SOUZA DELGADO

ERIKSON LUAN DA SILVA LIMA

IVANEIDE GONZAGA SALES

O AVANÇO NA COLETA DE DADOS, SEU IMPACTO PARA O MEIO TECNOLÓGICO E OS PROFISSIONAIS DE SEGURANÇA DE REDES

Trabalho Conclusão de Curso apresentado ao Centro Universitário Brasileiro – UNIBRA, como requisito parcial para obtenção do título de tecnólogo em Redes de Computadores.

Professor(a) Orientador(a): Msc Ameliara Freire Santos de Miranda
Professor(a) Co-Orientador(a): Aline Ferreira Barbosa Diego Ribeiro
Gomes

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 1745.

D352a Delgado, Diogo Souza

O avanço na coleta de dados, seu impacto para o meio tecnológico e os profissionais de segurança de redes / Diogo Souza Delgado, Erikson Luan da Silva Lima, Ivaneide Gonzaga Sales. Recife: O Autor, 2021.

22 p.

Orientador(a): Msc. Ameliara Freire Santos Miranda.

Trabalho De Conclusão De Curso (Graduação) - Centro
Universitário Brasileiro – Unibra. Tecnólogo em Redes de Computadores,
2021.

Inclui Referências.

1. Lei geral de proteção de dados. 2. Segurança da informação. 3. Tratamento de dados. I. Lima, Erikson Luan da Silva. II. Sales, Ivaneide Gonzaga. III. Centro Universitário Brasileiro - Unibra. IV. Título.

CDU: 004

Nossos imensos agradecimentos às nossas famílias, que nos deram todo apoio e força para a realização desse curso.

Aos nossos amigos, que batalharam conosco e nos acompanharam até a conclusão do mesmo.

Aos Professores, excelentes mestres da educação que contribuíram para nosso aprendizado.

AGRADECIMENTOS

Primeiramente somos grato a Deus, pela força que nos concede para não desistimos dessa caminhada, e por nos ajudar nas dificuldades que houveram no caminho.

Em especial, sou grata a minha querida avó que não está mais aqui, mas que antes de ir me ensinou valores e colaborou para eu me tornasse a mulher que sou hoje. Vó, eu sou a primeira a me formar!

Minha querida filha, você é parte essencial dessa caminhada. É por você que levanto todos os dias. Te amo muito!

Sou grata aos meus pais que me incentivaram. “Painho”, espero que o senhor esteja me vendo aí de cima e que esteja dando pulos de alegria.

Mãe, obrigada por me colocar neste mundo. Que Deus a abençoe.

Agradeço a minha Orientadora Ameliara Freire e minha Co-orientadora Aline Ferreira, por sempre estarem presente para nos direcionar de forma correta. Contribuindo para que esse trabalho fosse concluído com precisão.

Agradeço a todos os meus professores do fundamental até faculdade, sem vocês seria impossível concretizar minha graduação. Vocês são os responsáveis por todo meu aprendizado, porque ensinar é um dom que poucos tem a sorte de possuir.

Muito obrigada por tudo!

(Gonzaga, Ivaneide.)

SUMÁRIO

1. Introdução	8
2. A LGPD	9
2.1 <i>Da aplicabilidade da LGPD</i>	12
3. Segurança a Informação	14
3.1 <i>Integridade</i>	15
3.2 <i>Disponibilidade</i>	15
3.3 <i>Confidencialidade</i>	15
4. Conceitos de tratamento de dados	15
4.1 <i>DPO e sua importância para implementação da LGPD</i>	17
4.2 <i>DPO x Privacidade</i>	17
5. Ataques Cibernéticos	18
5.1 <i>Exemplos de Ataques Cibernéticos</i>	18
5.1.1 <i>Ataques de Malwares</i>	18
5.1.2 <i>Phishing</i>	19
5.1.3 <i>Manipulação de URL</i>	19
5.1.4 <i>Ransomware</i>	19
5.1.5 <i>Cavalo de Tróia</i>	19
5.2 <i>Como se proteger de ataques Cibernéticos</i>	20
5.2.1 <i>Firewall</i>	20
5.2.2 <i>Pentest</i>	20
5.2.3 <i>Gestão de Vulnerabilidade</i>	20
6. Considerações Finais	20
7. Referências	21

O AVANÇO NA COLETA DE DADOS, SEU IMPACTO PARA O MEIO TECNOLÓGICO E OS PROFISSIONAIS DE SEGURANÇA DE REDES

Diogo Sousa Delgado

Erikson Luan Da Silva Lima

Ivaneide Gonzaga Sales

Resumo:

O presente trabalho tem como objetivo apresentar alguns tópicos importantes sobre a Lei Geral de Proteção de Dados, sancionada em 2018. Um tema importante para sociedade brasileira que deve impulsionar a integração do setor de Tecnologia da Informação com os demais departamentos das empresas. A lei já está em vigor e possui a finalidade de intensificar o controle e o manuseio das informações que hoje circulam sem uma devida atenção em diversas organizações de direito público ou privado.

Palavras-Chave: Lei Geral de Proteção de Dados, Segurança da Informação, Tratamento de Dados.

1. INTRODUÇÃO

Desde que a Lei nº 13.709/2018 Geral de Proteção de Dados (LGPD) foi sancionada, o Brasil passou a unir-se a vários países onde já vigora legislação semelhante. O Brasil já contava com algumas leis que protegiam alguns dados de pessoas físicas e jurídicas, agora possui uma lei mais específica sobre o tema. O avanço da tecnologia de armazenamento de dados, trouxe facilidades para as empresas do meio tecnológico armazenar seus dados. Observa-se que essa mesma explosão tecnológica impôs limites principalmente éticos no que se refere a armazenamento de informações pessoais.

A extração de informações ocorre a todo tempo, tanto que a coleta de dados sofreu um enorme crescimento nos últimos anos. Nesse contexto, este trabalho abordará o impacto que a LGPD trará a Tecnologia da Informação e os profissionais em segurança de redes.

Há poucos anos atrás a extração de informações era bem mais difícil, pois o volume de dados da rede era bem menor, e os algoritmos não tinham seu desenvolvimento capaz de procurar com precisão a nível de detalhes

A grande vantagem do Brasil fazer parte dos países que possuem LGPD está na possibilidade de garantir, ao usuário, privacidade e controle de seus dados pessoais. Por isso, a lei estabelece detalhadamente os direitos do usuário, que é ponto fundamental da LGPD, a qual deve garantir parâmetros para a fiscalização e manutenção do mesmo, mantendo o usuário com o controle de seus dados nas mãos de terceiros.

A LGPD vem para melhorar a situação do tráfego de dados já que temos uma sociedade hiperconectada pelo grande avanço das tecnologias cada vez mais acessível à população, gerando assim um grande aumento no volume de dados gerados, algo que atualmente tem uma grande importância e valor a nível de informação.

O objetivo da LGPD lei sancionada em 14 de agosto de 2018, pelo ex-presidente Michel Temer, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

(<https://www.serpro.gov.br/lgpd> Online)

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Neste trabalho vamos analisar as dificuldades da implementação da LGPD nas empresas e como isso irá influenciar na vida do profissional de redes de computadores.

1.2.2 Objetivos Específicos

- Apresentar a LGPD;
- Detalhar o processo de aplicabilidade da LGPD.
- Demonstrar a importância da capacitação dos profissionais de redes para facilitar sua adaptação frente às novas diretrizes exigidas pela LGPD;

2. A LGPD

Com o passar dos anos, com os avanços tecnológicos e a inserção de novas tecnologias, como câmeras fotográficas, e a crescente invasão da vida privada pelas mídias, por exemplo, percebeu-se a necessidade de se consagrar um direito à privacidade com uma maior abrangência, ou seja, não respaldando apenas os meios físicos, conforme na época da Constituição do Império, mas sim uma extensão, em que esses direitos fossem um direito geral do indivíduo. Assim, se poderia escolher em qual extensão desejariam comunicar os seus pensamentos, os seus sentimentos e a suas emoções para os outros. Desse modo, em 1890 foi publicado, na Harvard Law Review, um artigo denominado “The Right to Privacy”, em tradução livre “O Direito à Privacidade”, que abrangia a necessidade de um direito à privacidade mais abrangente, evidenciando que a privacidade “é o direito de ser deixado em paz” (WARREN,1890).

Para compreensão de toda lei é preciso conhecer as definições e conceitos, sobretudo porque a grande maioria está sendo apresentada à LGPD pela primeira vez. (Rafael Fernandes 2020 p.22)

Conforme coceitua Rafael Fernandes na sua obra “Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais”, a LGPD é uma Lei que:

Dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade natural, inclusive por meio digital. (FERNANDES, 2020, p. 17).

Também pode-se dizer que a LGPD trata da proteção aos dados coletados ou processados de alguma forma. Protegendo a privacidade dos cidadãos, sejam eles brasileiros ou estrangeiros que estão no Brasil, buscando sempre um equilíbrio entre os novos modelos de negócios que vêm surgindo cada vez mais com o avanço das tecnologias e a globalização. Com relação ao uso e à proteção da privacidade desses dados coletados, esse é um direito cada vez mais em pauta pelos cidadãos.

A LGPD na Lei nº 13.853/2019, no Artigo 2º tem como fundamentos para a devida utilização dos dados pessoais:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

- I - O respeito à privacidade;**
- II - A autodeterminação informativa;**
- III - A liberdade de expressão, de informação, de comunicação e de opinião;**
- IV - À inviolabilidade da intimidade, da honra e da imagem;**
- V - O desenvolvimento econômico e tecnológico e a inovação;**
- VI - A livre iniciativa, a livre concorrência e a defesa do consumidor;**
- VII - Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.**

(www.planalto.gov.br)

Depois de analisar os principais artigos da Lei Geral de Proteção de Dados, pode-se observar que a Lei não tem apenas como objetivo proteger a privacidade dos usuários, mas trazer crescimento, desenvolvimento para setor econômico e tecnológico, podendo assim proporcionar tranquilidade para empresas, clientes e funcionários.

De fato isso é algo real, pois poucos sabem como a LGPD irá afetar de tal forma da coleta de dados e tratamentos de dados após a implementação da LGPD no Brasil. Contudo levará um certo tempo para as pessoas e empresas se adequarem lei.

Em relação ao tratamento de dados o que define Rafael Fernandes “definição trazida pela LGPD tira do imaginário de muitos a premissa de que estariam fora do alcance da nova legislação”.

Entende-se que a LGPD é uma lei que tem como objetivo prezar pela privacidade do usuário e qualquer dado pessoal utilizado seja ele individual ou não, e como todas essas ações podem identificar através de pessoa responsáveis as que são o controlador e operador.

A LGPD é um divisor de águas na proteção de dados e tratamentos de dados sua importância é algo totalmente fundamental nos dias de hoje onde os dados são informações muito sensíveis e super importantes para haver qualquer tipo de descuido ou negligência sobre ela.

E pode-se ser acrescentando o fato de que com o aumento da tecnologia e as suas falhas muitos bancos de dados sem nenhum investimento robusto em segurança deixa não apenas os dados pessoais vulnerável como os dados da própria empresa,

Destaca-se também que o Brasil participa de alguns acordos internacionais que já possuem considerações, ainda que rasas, sobre a proteção de dados pessoais, como a Convenção de Berna de 1886 e o Acordo sobre Aspectos dos Direitos de Propriedade Intelectual relacionados ao Comércio (TRIPS). Da mesma forma, algumas leis internas do país também têm breves passagens sobre o tema, são elas o Código de Defesa do Consumidor (art. 43º), o Marco Civil da Internet (art. 7º e 11º) e o Decreto sobre Comércio Eletrônico (art. 4º).

13 Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Brasília, DF

14 Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

- a) justifiquem sua coleta;
- b) não sejam vedadas pela legislação; e
- c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet.

2.1 Da aplicabilidade da LGPD

A LGPD é aplicável a todos que realizam o tratamento de dados pessoais, sejam elas pessoas de direito público ou privado, pessoa física ou jurídica, desde que estejam realizando qualquer tipo de operação que se enquadre no tratamento dos seus dados. Isso ocorre independentemente do meio, do país da sua sede ou da nação em que estejam localizados os dados, desde que: a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens, serviços ou o tratamento de dados de indivíduos localizados no território nacional; os dados pessoais objeto do tratamento tenham sido coletados no território nacional conforme expresso no artigo 3º, I, II e III da Lei 13.709/2018 (LGDP).

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional.

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Outro ponto que vale destacar é no sobre a extraterritorialidade da lei. Desde que os dados tenham sido coletados em território nacional, até mesmo por oferta de produto ou serviço para pessoas no território nacional ou que estivessem no Brasil, a LGPD será aplicada com efeitos internacionais. Simplificando, caso uma empresa colete dados pessoais no território nacional, porém a sua sede seja em outro país, essa organização, terá que se enquadrar nos termos da LGPD.

Mais um ponto a ser observado é referente ao artigo 4º da LGPD:

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

É possível observar que a lei trouxe uma certa limitação de aplicabilidade em relação aos tipos de dados que são regulados pela LGPD. “O tratamento de dados pessoais deve seguir um propósito certo e funcional, mas que não supere a liberdade de informação e expressão, a soberania, a segurança e a defesa do Estado.” Têm-se, nesse sentido, uma certa limitação, buscando consigo uma maior segurança em temas relevantes da sociedade.

(Patricia Peck 2018, p. 43-44)

Outro ponto que vale a atenção sobre a LGPD é o fato de que a lei se aplica apenas nos casos que existe a busca da oferta ou do fornecimento de bens ou serviços, ou seja, quando há uma questão econômica por trás. Nos casos em que não há esse propósito e quando se trata de uma pessoa natural, não se fala em aplicação da LGPD.

O que a Lei busca de forma direta com essa especificação é a proteção dos dados pessoais, que se tornou, nestes últimos tempos, uma moeda muito valiosa para troca pelos usuários para ter acesso a determinados bens, serviços ou conveniências.

3. SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação deve estar presente em toda empresa e organização que desejam manter suas informações em segurança.

Quando falamos em segurança da informação o que se pretende afirmar é que se trata da proteção de dados contra ataques e vazamentos. (NBR ISO/IEC 27002:2005).

“Ao falar em segurança da informação deve-se considerar levar em essas qualidades da informação, pois toda ação que venha a comprometer qualquer uma dessas qualidades estará atentando contra a sua segurança”.
(Marcus Leal, p13, 2001)

As qualidades são: Integridade, disponibilidade e confidencialidade.

3.1 Integridade

A integridade é a garantia da exatidão e completeza da informação dos métodos de processamentos de dados (NBR ISO/IEC 27002:2005).

Para garantir integridade dos dados, é necessário assegurar que não seja permitido nenhum tipo de alteração da informação sem autorização, como: exclusão, modificação ou destruição de dados e informações.

Caso aconteça alguma dessas ações é considerada a quebra de integridade, pois a informação foi alterada.

3.2 Disponibilidade

A disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário (NBR ISO/IEC 27002:2005)

O que pode ser considerado uma quebra de disponibilidade é a negação do alcance às informações e dados quando necessário.

Isso ocorre quando informações e dados não podem ser acessados pelos usuários e destinatários, ou seja, não há possibilidade de consulta da informação dos dados quando for necessário.

3.3 Confidencialidade

A confidencialidade é a garantia de que a informação é acessível somente por pessoas autorizadas. (NBR ISO/IEC 27002:2005).

Pode-se considerar uma quebra de confidencialidade quando pessoas que não possuem a autorização necessária conseguem ter acesso a informações e dados. Assim, é possível afirmar que a perda da confidencialidade é o vazamento de informações de dados que deveriam estar completamente protegidos.

4. CONCEITOS DE TRATAMENTO DE DADOS

Tratamento de dados toda operação que é realizada com dados pessoais. Pode-se dizer que o tratamento de dados é composto por algumas etapas que divididas em 5 operações como mostra a figura a tabela abaixo:

Etapas de tratamento de dados	Operações de tratamento 5 X art LGPD
Coleta	Coleta, produção, recepção.
Retenção	Arquivamento e armazenamento.
Processamento	Utilização, reprodução, classificação, processamento, avaliação ou controle da informação, extração e modificação.
Compartilhamento	Distribuição, transmissão, comunicação, transferência e difusão.
Eliminação	Eliminação (término do tratamento de

	dados)
--	--------

(<https://legalcloud.com.br>)

“O tratamento de dados apresenta o conjunto de operações que estão sob a tutela da LGPD para que seja efetivada a proteção de dados, logo, a importância de fazer um tratamento de dados pessoais adequado à Lei “.

Assim, se houver qualquer ação com dados, mesmo que não esteja presente na tabela apresentada, provavelmente ela estará sendo processada.

Portanto, a importância do tratamento de dados pessoais de acordo com a legislação é enorme e os DPO são os profissionais essenciais para as empresas cumpram o que é pedido pela nova LGPD.

Precisamente porque o conhecimento sobre LGPD está cada vez mais em demanda, e as empresas precisam adequar-se à Lei.

**GROSSI, Bernardo. “Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 Porto Alegre, RS: Editora Fi, 2020.
Guia de Boas Práticas – Lei Geral de Proteção de Dados (LGPD)” do Governo Federal <https://legalcloud.com.br>**

4.1 DPO e sua importância para implementação da LGPD

O DPO ou Data Protection Officer é o profissional contratado por uma empresa e se dedica exclusivamente à LGPD. Com a vigência da LGPD no Brasil as empresas tiveram que criar o cargo de DPO e contratar um profissional.

4.2 DPO x Privacidade

Quando falamos em DPO, transparência e privacidade nos referimos à necessidade de deixar claro para o cliente quais dados irão ser coletados pela empresa ou organização e, ainda, como eles serão usados, tratados e armazenados.

“Sua utilização, então, implica no consentimento da parte que fornece os dados e confia na empresa ou organização e o DPO é responsável por garantir a privacidade e segurança deles”. (fia.com.br/blog, 2020, online)

Então entende-se que o profissional *Data Protection Officer* deve garantir que o cliente tenha total acesso aos dados coletados de forma transparente e estar ciente de qual forma será feito o uso deles.

5. ATAQUES CIBERNÉTICOS

Os ataques cibernéticos estão acontecendo de forma mais comum do que podemos imaginar. Eles acontecem a partir de softwares maliciosos, mais conhecidos como malware e podem afetar todos os dados das empresas ou pessoa física. Podendo até mesmo provocar falha em aparelhos e máquinas, gerando prejuízos. Além desse tipo de ataque, pode ocorrer a invasão de privacidade, o roubo de informações, fraudes e clonagens.

A cada dia que passa cresce o uso de tecnologias e, proporcionalmente, as formas dos crimes cibernéticos, inclusive com bastante engenhosidade. Podendo ser comparado até com crime de fora do mundo virtual. Em empresas, isso pode gerar prejuízos envolvendo milhões de reais.

As notificações referentes a ataques cibernéticos contra empresas brasileiras cresceram 220% no primeiro semestre deste ano em comparação com o mesmo período de 2020. Os dados foram divulgados na pelo grupo Mz, empresa especializada em relações com investidores, com base em dados levantados pela Comissão de Valores Mobiliários (CVM), agência regulada pelo Ministério da Economia. (<https://www.cnnbrasil.com.br/business/ataques-ciberneticos-a-empresas-brasileiras-crescem-220-no-1-semestre-de-2021/>)

5.1 EXEMPLOS DE ATAQUES CIBERNÉTICOS

5.1.1 Ataques de Malwares

O ataque ocorre quando o sistema ou a rede ampla de computadores acaba sendo infectada por um malware. A máquina afetada pode ser usada pelo cibercriminoso para diversos fins. Roubo de dados confidenciais e usar a máquinas como pontos para a realização de outros crimes são dois exemplos.

5.1.2 Phishing

O phishing é usado durante o aproveitamento da confiança do usuário, assim sendo possível roubar seus dados. O cibercriminoso finge ser uma pessoa ou até mesmo uma empresa para enganar as vítimas. Pode ocorrer de várias maneiras, tanto por conversas em aplicativos de comunicação, quanto por e-mails fraudulentos.

5.1.3 Manipulação de URL

O usuário faz uso apenas do link que é dado pela página do site. Se ele alterar de forma manual a URL, ele pode ter diversas combinações até chegar a um endereço que esconde uma área restrita apenas para autorizados. O cibercriminoso pode fazer o ter acesso a essa parte privada usando caracteres que não são esperados pelo desenvolvedor. Assim a página envia uma mensagem de erro que pode revelar várias informações sigilosas.

5.1.4 Ransomware

Trata-se de um malware “sequestrador”. Todos os dados vulneráveis são sequestrados e, então um valor é cobrado como forma de resgate. Muito semelhante ao mundo real.

Esse malware pode deixar a empresa parada por dias, prejudicando sua produtividade. É importante sempre ter boas ferramentas para deter esse tipo de ameaça, e manter todo o sistema atualizado.

5.1.5 Cavalo de Tróia

O Trojan, mais conhecido como Cavalo de Tróia é o malware mais comum e afeta os computadores de todo o mundo. Ele executa um código nas máquinas afetadas e as deixam vulneráveis, servindo de porta para outros malwares e ataques de cibercriminosos.

Ele costuma vir em formato executável (programa), as vítimas, sem saberem, fazem o download e logo a máquina é afetada.

5.2 COMO SE PROTEGER DE ATAQUES CIBERNÉTICOS

As melhores formas de evitar invasões é sempre ter um bom antivírus, manter o sistema sempre atualizado e fazer manutenção nas redes. Toda empresa e até mesmo pessoas estão sujeitas a ataques cibernéticos. Podendo acontecer a qualquer momento do dia, com qualquer descuido, por isso é sempre importante adotar medidas de segurança.

5.2.1 Firewall

O firewall é o dispositivo mais básico e mais usado entre empresas e usuários comum. Ele serve como uma proteção extra, funcionando muito bem em conjunto com um antivírus.

5.2.2 Pentest

Funciona como uma prevenção. Ele visa corrigir e eliminar todo tipo de vulnerabilidade dos computadores, impossibilitando invasões de cibercriminosos.

5.2.3 Gestão de Vulnerabilidade

A gestão de Vulnerabilidades vai funcionar igual uma central de gerenciamento. Ela é capaz de coletar dados, identificar e monitorar várias fontes para ver se são seguras. As brechas de invasões surgem a todo momento, então a gestão vai servir para evitar que isso aconteça, deixando as empresas sempre protegidas.

6. CONSIDERAÇÕES FINAIS

Podemos afirmar que a implementação de uma Lei que visa garantir a regulamentação de todo o tratamento de dados pessoais dos cidadãos brasileiros dentro e fora do Brasil é de suma importância.

Atualmente, a LGPD é uma das leis mais importantes em processo de implementação no Brasil, uma lei que tem a finalidade de regulamentar a forma de lidar com a proteção de dados pessoais dos cidadãos brasileiros, o seu impacto é diretamente ligado a qualquer organização presente no território nacional.

Quanto a forma de lidar com dados pessoais, corporativos, bem como os dados de terceiros, a LGPD está em conformidade com o GDPR, a Lei Regulamentadora da União Europeia e de todo o seu espaço econômico, uma vez que está sendo aplicada nos países pertencentes à União. Essa maneira de lidar e processar os dados, é muito importante já que os regulamentos existentes não cobriam tudo, apenas adotavam algumas medidas de privacidade e segurança de dados, medidas essas que muitas das vezes foram violadas por empresas que usufruíram dos dados de cidadãos para influenciar e comercializar informações dos mesmos ao redor do mundo.

Como fundamentos da LGPD podemos destacar o respeito à privacidade, liberdade de expressão, inviolabilidade da intimidade, livre iniciativa, defesa do consumidor, direitos humanos, dignidade e exercício da cidadania. Na prática, a LGPD se aplica aos governos e às empresas, tendo que garantir maior segurança aos dados pessoais, sempre observando a finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, responsabilização e a prestação de contas de tudo que se refere aos dados pessoais.

De forma geral, conforme mostrado neste trabalho, os pontos mais importantes do panorama geral da LGPD podem ser sintetizados da seguinte forma: a LGPD é uma regra para todos, ou seja, cria um cenário de segurança jurídica válido para todo o país; estabelece de maneira clara, o que são os dados pessoais e como deverá ser feito o devido tratamento deles; como regra, para que os dados pessoais possam ser tratados, deve haver o consentimento do seu titular, tendo como exceção apenas os casos em que seja indispensável cumprir critérios legais; não importa se a organização ou o centro de dados estão dentro ou fora do Brasil, sendo a sua abrangência extraterritorial, conforme bem pontuado durante o trabalho; no caso de inobservância da legislação, há aplicação de penas rígidas; a lei traz consigo definições de que são dados pessoais indispensáveis ao bom entendimento da legislação; a lei evidencia as responsabilidades de cada agente de tratamento e as suas funções.

REFERÊNCIAS

BRASIL, Lei nº13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

Marciel, R.M. Manual prático sobre a Lei Geral de Proteção de Dados Pessoais. Independently Published, 22 abril 2019, 170 páginas.

BRASIL. *Marco Civil da Internet*. Brasília, DF: Congresso Nacional, 2014.

PINHEIRO, Patricia Peck. *Proteção de dados pessoais – Comentários à Lei N. 13.709/2018 (LGPD)*. São Paulo: Saraiva Educação, 2018.

EUROPA. Regulamento (EU) 679/2016. Disponível em <<https://op.europa.eu/pt/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1>>. Acesso em 23 de agosto de 2021.

AVAST. Crimes Virtuais. Disponível em <<https://www.avast.com/pt-br/cybercrime>>. Acesso em 29 de agosto de 2021.

MORGAN, Steve, CYBERCRIME MAGAZINE. Disponível em <<https://cybersecurityventures.com/cybersecurity-almanac-2019/>>. Acesso em 09 de setembro de 2021.

SOPRANA, Paula. Cresce demanda por especialistas em privacidade. 16 set. 2018. Disponível em <<https://www1.folha.uol.com.br/mercado/2018/09/cresce-demanda-porespecialistas-em-privacidade.shtml>>. Acesso em 09 de setembro de 2021.

SERPRO. Os 10 princípios para um efetivo tratamento de dados, segundo a Lei Geral de Proteção de Dados Pessoais. Disponível em <https://www.serpro.gov.br/lqpd/menu/arquivos/os-10-principios-para-um-efetivotratamento-de-dados/view>. Acesso em 17 de setembro de 2021.

THE ECONOMIST. O recurso mais valioso do mundo não é mais petróleo, mas dados: Regulando os gigantes da Internet. The Economist. Londres, 06 maio 2017. Disponível em: <<https://www.economist.com/leaders/2017/05/06/the-worlds-mostvaluable-resource-is-no-longer-oil-but-data>>. Acesso em 02 de outubro de 2021.

ALBERTIN, A. L.; ALBERTIN, R. M. M. Dimensões do uso de tecnologia da informação: um instrumento de diagnóstico e análise. *Revista de Administração Pública*, v. 46, n. 1, p. 125-151, 2012.

GIL, Antônio Carlos. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2002.

www.gov.br/defesa/pt-br/aceso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lqpd. Acesso em 17 de setembro de 2021