LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E A UTILIZAÇÃO DA COMPUTAÇÃO EM NUVEM

GENERAL DATA PROTECTION ACT (LGPD) AND THE USE OF CLOUD COMPUTING

Débora Gomes Almeida

Rogério Oliveira da Silva

RESUMO

Muitas pessoas desconhecem sobre a Lei Geral de Proteção de Dados, ocasionando em problemas devido à má utilização de informações. O objetivo deste artigo é apresentar as aplicações corretas de medidas de mitigação, uma contextualização sobre o assunto, ou seja, estar totalmente pronto para a regulamentação de proteção de dados. A computação em nuvem é uma inovação que permite que as empresas controlem serviços de maneira descentralizada, onde todos os dados ficam armazenados na internet, obtendo assim agilidade e acesso aos dados a qualquer momento, de qualquer lugar. Contudo, existem alguns desafios a serem superados na corrida por conformidade com a lei, essa tecnologia deve ser gerenciada, com foco nos pontos mencionados e nos pilares da segurança da informação.

Palavras-chave: LGPD; Computação em nuvem; Armazenamento de dados; Proteção de Dados; Direitos do titular.

ABSTRACT

Many people are unaware of the General Data Protection Law, causing problems due to misuse of information. The purpose of this article is to present the correct applications of mitigation measures, a contextualization on the subject, that is, to be fully ready for data protection regulation. Cloud computing is an innovation that allows companies to control services in a decentralized manner, where all data is stored on the internet, thus obtaining agility and access to data anytime, from anywhere. However, there are some challenges to be overcome in the race for compliance with the law, this technology must be managed, focusing on the points mentioned and the pillars of information security.

Keywords: *LGPD; Cloud computing; Data storage; Data Protection; Rights of the holder;*

Introdução

A Lei Geral de Proteção de Dados (LGPD) de Nº 13.709/2018, foi criada para garantir que pessoas físicas ou jurídicas tomem as devidas providencias para estabelecer a proteção dos dados pessoais, quando eles serem coletados, tratados, armazenados e protegidos. Em congruência com a legislação do grupo de países que

adotam uma Lei Geral de Proteção de Dados, o regimento jurídico interno fora inspirado pela regulamentação vigente na Europa (General Data Protection Regulation – GDPR), que objetiva justamente a proteção e privacidade dos dados de todos os indivíduos da União Europeia e Espaço Econômico Europeu.

Os dados pessoais estão em todos os lugares, desde as centrais de atendimento, instituições bancárias, redes sociais, farmácias. Antes da LGPD, eram implementadas medidas de segurança da informação sem a devida proteção dos dados pessoais, porém agora se torna obrigatório tomar as devidas providências para estabelecer a proteção dos dados pessoais.

A Constituição Federal (1988, Art. 5º, Inciso X) entende que:

> São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. A lei também estabelece punições para descumprimento em casos de vazamentos, ou outras irregularidades.

Os principais objetivos da lei se resumem ao: Respeito à Privacidade, onde as empresas precisam respeitar o titular dos dados, a legislação e objetivos que ela coloca. A livre Iniciativa e o Desenvolvimento Econômico, onde concede as empresas já regulamentadas uma grande vantagem competitiva as que ainda não se adequaram corretamente. Os Direito Humanos que concedem uma retratação caso algum incidente cause embaraço ou constrangimento ao titular. Autodeterminação Informativa e Liberdade de Expressão, fazendo com que as empresas respeito a sua finalidade ao informar seus dados em qualquer ambiente.

Todo e qualquer dado de indivíduos localizados no Brasil, sendo ou não brasileiro, mas que passe pelo território, está abaixo da LGPD e sob proteção. Ao realizar troca de dados com outros países é importante verificar se ele possui uma proteção semelhante a que a Lei resguarda, caso contrário o indivíduo poderá responder por qualquer incidente que cause.

A lei não se aplica a tratamentos realizados para fins exclusivos de: Segurança pública, Defesa nacional, Segurança do estado, Acadêmicos, jornalísticos e artísticos, onde estes dados são utilizados para investigações, pesquisas, estatísticos ou trabalhos culturais.

2. Direitos do titular

Todo titular possui o direito de saber se seus dados pessoais estão armazenados em qualquer empresa. Confirmando a existência ele poderá ter acesso a estes dados e realizar algumas mudanças. Exemplo:

1. Pedir a correção caso tenha algum erro;
2. Anonimização ou bloqueio de dados desnecessários;
3. A eliminação dos dados quando for possível, isto porque as empresas também têm seus direitos tributários de guardar dados, respeitando as bases legais.
4. Portabilidade dos dados a outro fornecedor de serviço ou produto;
5. Informações das entidades com as quais o controlador realizou o uso compartilhado de dados;
6. Informações sobre a possibilidade de não fornecer consentimento;

7. Revogação do consentimento se irregular;
8. Oposição ao tratamento, se irregular;
9. Reclamação a Autoridade Nacional.

3. Dados Pessoais

A LGPD trata de dados pessoais, que é uma informação relacionada a pessoa natural identificada ou identificável. Exemplo: Nome do titular, endereço de residência, cpf, rg, número de um cartão de identificação, endereço de IP, cookies etc. Porém existe outros tipos de dados, que são:

1. Dado pessoal indireto, onde possui informações que não podem relacionar diretamente um indivíduo, porém, unidas a outras podem identificá-lo. Exemplo: Uma placa de carro, dados do cônjuge, características físicas únicas em um grupo de pessoas;
2. Dado pessoal sensível: Precisa ter um cuidado especial sobre eles, pois podem trazer de alguma maneira discriminação o prejuízo ao titular. Exemplo: cor, raça, opção sexual, opinião política etc.
3. Dado anonimizado: Dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis para o tratamento. A lei não considera como um dado pessoal, neste caso é orientado a minimizar.
4. Dados não pessoais: Não são observados pela LGPD, não são considerados dados pessoais. Exemplo: Dados corporativos, estatísticas, dados de natureza pública etc.
5.

4. Bases Legais de Tratamento

A base legal permite que os dados pessoais sejam coletados e tratados, até independente da vontade do titular. Utilizamos como exemplo as leis trabalhistas que exigem que os dados de funcionários sejam armazenados por um período que varia de 5 a 20 anos, de acordo com o documento (Portaria SPREV nº 211/2019).

As bases legais também concedem aos seguintes âmbitos:

1. O Poder Público, poderá coletar dados pessoais, desde que eles sejam utilizados para atender as finalidades específicas e claras de políticas públicas, de preferência, divulgadas em seus sites. Exemplos: Vacinação, segurança, investigação etc. Lei nº 13.709, Inciso III, de 14 de agosto de 2018:

> Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei.

2. Os órgãos de pesquisa (IPEA, IBGE, Embrapa etc.) são permitidos pela Lei LGPD de coletar dados pessoais, utilizando sempre que possível, técnicas de anonimização ou pseudonimização de dados sensíveis. Segundo o Art. 13º da Lei nº 13.709, de 14 de agosto de 2018:

> Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas

de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

3. No ambiente jurídico, o exercício regular de direito é defendido pela realização de ações de acordo com a legalidade de um ponto de vista objetivo, ou seja, se você estiver em uma atividade de exercício regular de direito envolvendo dados pessoais, poderá ser realizado até mesmo sem autorização do titular. Exemplo: Médico em uma cirurgia realiza um corte no paciente, ele não responderá criminalmente por lesão corporal, pois essa ação foi extremamente necessária.
4. A coleta dos dados pessoais é permitida também nos casos de proteção da vida do titular do dado. Exemplo: Você sofre um acidente e é encaminhado para tratamento, o hospital então colherá seus dados pessoais para avisar os seus familiares, verificar se possui alguma alergia ou determinada religião que proíbe determinados tratamentos médicos.
5. O legítimo interesse do controlar é quando o titular solicita um serviço que o beneficie, desde que respeite as suas expectativas. Exemplo: Ao solicitar a abertura de uma conta bancária, o titular precisa informar seus dados pessoais para que a devida conta seja aberta e validada com sucesso.
6. A proteção ao crédito, concede o direito a empresa no qual o titular possui pendências de pagamento, disponibilizar sem a sua permissão os dados pessoais para os Órgãos de Proteção ao Crédito (SPC/SERASA), impedindo o titular de solicitar sua exclusão enquanto a dívida não for liquidada.
7. O consentimento, onde o titular demonstra, por meio de contrato escrito ou outro meio que demonstre a manifestação da vontade do titular, que está ciente de como os dados serão coletados e utilizados pelo controlar, após clara exposição da finalidade, caso não seja feito a empresa poderá ser penalizada. A lei também autoriza ao titular a revogação o consentimento ou exclusão, a qualquer momento.

5. Tratamento de Dados Pessoais

Tanto o GDPR quanto a LGPD exigem que os controladores estabeleçam uma base legal para tratar dados pessoais. Essas leis possui bases semelhantes, porém enquanto o GDPR estabelece seis bases legais, a LGPD permite dez bases legais.

Segundo o Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

1. Finalidade: Processar para propósitos legítimos, específicos, explícitos e informados ao titular, ou seja, quando for fornecido o dado para uma instituição, ela deverá explicar o motivo deste fornecimento;
2. Adequação: Compatibilidade do tratamento com as finalidades informadas ao titular. Não poderá ser coletado dado para determinada finalidade e depois realizar alterações;
3. Necessidade: Limitação do tratamento ao mínimo necessário para a realização de suas finalidades.
4. Livre acesso: Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento.
5. Qualidade dos dados: Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados.

6. Transparência: Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre o tratamento e envolvidos.
7. Segurança: Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais. De acordo com a necessidade da empresa, serão aplicadas as medidas de segurança;
8. Prevenção: Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
9. Não discriminação: Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
10. Responsabilização: Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a conformidade.

6. Ciclo de Vida dos Dados Pessoais

Depois de ter ciência de quais são os dados pessoais e as atividades de tratamento, pode-se compreender o ciclo de vida destes dados. Após a publicação da lei de proteção, ocorreram mudanças nas seguintes fases do ciclo:

1. Coleta: Os dados coletados que se transformarão em informação e devem obedecer aos princípios;
2. Processamento: Só será realizado, se houver uma forma de consentimento pelo titular dos dados ou outra base legal;
3. Análise: Deverá levar em consideração, os regulamentos da proteção de dados, obedecendo aos princípios da finalidade e da necessidade de tratamento para os propósitos legítimos, específico e explícito;
4. Publicação: Será válida para os dados que são tornados públicos pelo titular.
5. Armazenamento: Os dados devem possuir prazos de tratamentos definidos, sendo necessários assim verificar se a finalidade ou os dados deixaram de ser necessários, aplicando assim as medidas de exclusão, anonimização ou pseudonimização;
6. Exclusão: Os dados coletados deverão ter prazos definidos para exclusão/destruição e devem seguir procedimentos mapeados para excluir cada tipo de dado;
7. Reutilização: Com a finalidade alcançada no uso de dados, estes não podem ser reutilizados para qualquer outra finalidade sem o consentimento do titular.

7. Principais papéis

Os principais envolvidos no tratamento dos dados pessoais que a lei traz como tendo necessidade nas empresas são:

1. Titular: Pessoa que fornece/refere os dados pessoais;
2. Controlador: Responsável por coletar os dados, cuidar de todo controle, cuidado e proteção dos dados pessoais, identificar as vulnerabilidades e sanar eventuais riscos, regras de boas práticas de governança, informar ao titular as finalidades dos dados e tratamento utilizado, elaboração do Relatório de Impacto à proteção dos dados, comunicar a Autoridade Nacional e aos titulares em casos de ocorrências de incidentes de segurança que possa acarretar risco ou dano relevante aos titulares.

O Art. 48 entende que:

> O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
>
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
>
> I- A descrição da natureza dos dados pessoais afetados;
> II- As informações sobre os titulares envolvidos;
> III- A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> IV- Os riscos relacionados ao incidente;
> V- Os motivos da demora, no caso de a comunicação não ter sido imediata; e
>
> VI- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

O controlador e o operador de dados, deverão manter registros de todas as operações que realizarem, e serão solidariamente responsáveis pelos danos que causarem nos exercícios de suas atividades, respondendo civilmente e administrativamente.

1. Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. (Art.5º, VII). Processa os dados pessoais somente em instrução documentada do controlador, toma medidas de segurança apropriadas, auxilia o controlador por medidas técnicas e organizacionais apropriadas, disponibiliza ao controlador todas as informações necessárias para demonstrar o cumprimento das obrigações etc.
2. ANPD: É um órgão novo que foi criado para a aplicação da LGPD, onde realiza a fiscalização da aplicação da lei, esclarecimento de dúvidas e sancionar quando houver acidentes, elaborar diretrizes para a política nacional de proteção de dados pessoais e privacidades, as empresas deverão seguir etc.
3. Encarregado: Responsável por questões relacionadas a lei em nome do controlador, ponte entre o titular e o controlador, podendo ser interno, funcionário do quadro da empresa ou externo, garantindo que não haja qualquer conflito de interesse etc. “Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) ”. (Art.5º, VIII).

O Comitê de Privacidade e Proteção de Dados é um agente opcional interno, composto por facilitadores e responsáveis pela proteção dos dados e disseminação das informações. Ele irá auxiliar o encarregado em suas atribuições, auxiliar na implementação das mudanças a fim de mitigar riscos, auxiliar na conscientização dos colaboradores sobre a política de privacidade e proteção de dados, direitos, obrigações e coparticipação etc.

8. Vulnerabilidades

É uma condição que quando explorada por um atacante, pode resultar em um incidente. Dentro e fora de uma organização pode ocorrer ataques. Divulgação não intencional, dispositivos sem medidas de segurança apropriadas, descarte incorreto

de equipamentos e documentos podem resultar em exposição de dados, para isso os funcionários precisam ser capacitados para evitar este tipo de incidente.

Ataques maliciosos são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Uma vez instalados, eles passam a ter acesso aos dados armazenados e podem executar ações em nome dos usuários. Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo.

Em novembro de 2020, o Superior Tribunal da Justiça sofreu um ataque hacker, onde os invasores conseguiram criptografar toda a base de dados do tribunal, incluindo parte dos backups do sistema. O restabelecimento dos sistemas foi finalizado após 15 dias. No mesmo mês ocorreu outro ataque, no TRF-1, onde foram obtidas mais de 40 bases de dados como forma de demonstrar a “vulnerabilidade” na segurança do Tribunal. De acordo com o TRF-1, “todos os sistemas do tribunal foram colocados em modo restrito para permitir a adequada investigação”.

O acesso indevido sofrido a estes ambientes tecnológicos resulta em uma quebra direta de princípios enunciados pela LGPD, como o da segurança e o da prevenção de incidentes de modo geral. A jornada para a transformação digital e a necessidade dos negócios se ajustarem internamente para ficar em conformidade com as exigências da lei obrigam as empresas a buscar soluções de segurança de dados e redes na Nuvem, um exemplo de softwares é o Cloud computing ou computação em nuvem.

9. Computação em Nuvem

Computação em nuvem ou Cloud computing é uma tecnologia que permite o armazenamento de dados na Internet por meio de um provedor de computação na nuvem, que gerencia e opera o armazenamento físico de dados como serviço, obtendo assim agilidade e acesso aos dados a qualquer momento, em qualquer lugar. Justamente por não necessitar da instalação de programas, ou do armazenamento de dados, o conceito originado do inglês cloud computing faz alusão à “nuvem”. Atualmente existem três modelos de implantação em nuvem:

1. Nuvem privada: Recursos de computação em nuvem usados exclusivamente por uma única empresa ou organização. Uma nuvem privada pode estar localizada em seu data center local ou hospedada na nuvem por um provedor de serviços;
2. Nuvem pública: Toda infraestrutura pertence e são gerenciados por um provedor de serviços, logo o titular acessa seus documentos através de um navegador;
3. Nuvem híbrida: Combinação de nuvens pública e privadas para compartilhar dados e aplicações, conectando infraestrutura e aplicações entre recursos baseados em nuvem e recursos fora da nuvem.

Os três principais tipos de computação em nuvem são:

1. Infraestrutura como serviço (laaS): Oferece maior nível de flexibilidade e controle de gerenciamento, acesso a recursos de rede, computadores virtuais e espaço de armazenamento de dados;

2. Plataforma como serviço (PaaS): Foco voltada na implantação e no gerenciamento de aplicativos/
3. Software como serviço (Saas): Oferece um produto completo, executado e gerenciado pelo provedor de serviços. Na maioria dos casos, quando as pessoas mencionam SaaS, estão falando de aplicativos de usuários finais (como e-mail baseado na web).

10. Segurança no Armazenamento de Dados na Nuvem

O armazenamento em nuvem disponibiliza uma acessibilidade remota, implantação rápida e melhor facilidade de compartilhamento, ao contratar este serviço, sua empresa passa a contar com soluções avançadas de segurança, além de ferramentas capazes de detectar e evitar os mais diversos tipos de ameaças.

No dia a dia existem medidas importantes para adoção, como a criação de senhas envolvendo letras, números e caracteres especiais é de suma importância para que ela não seja descoberta, aliado a autenticação em duas etapas, pois caso você sofra uma tentativa de ataque, o sistema envia para seu e-mail ou celular cadastrado um código de confirmação e somente com ele você consegue acessar o serviço. A realização de backups garante a continuidade das operações internas, protegendo também de algum desastre natural.

É fundamental pesquisar sobre o fornecedor de serviço em nuvem, fiscalizar se ele realiza auditorias em relações a suas operações, o certificado de segurança utilizado, a criptografia codificada para que apenas o emissor e o receptor consigam interpretá-la. Ao contratar, realize o controle de acesso aos colaboradores aos diferentes níveis de informação, criando hierarquia e diminuindo o risco de vazamento de dados. Caso a prestadora de serviço vier a falir ou ser comprada por outra, o titular tem total liberdade e disponibilidade de revogar os seus direitos e migrá-los para outro fornecedor.

Conforme artigo publicado por Araújo (2020), a segurança cibernética não pode ser mais encarada como uma decisão que está à parte das inovações e operações do dia a dia do negócio. Para isso, no entanto, é preciso que as companhias avancem em seus planos de segurança, entendendo a LGPD e outras regras de conformidade digital

11. Ferramentas gratuitas de armazenamento

O armazenamento em nuvem é uma tecnologia vantajosa para os titulares e caso você não possua condições de contratar um fornecedor, existem ferramentas gratuitas que disponibilizam a proteção. O mais conhecido é o Google Drive, onde o titular insere seu e-mail do Gmail e já consegue utilizar os recursos oferecidos como: 15gb de espaços gratuitos, segurança no acesso a conta, definições de permissões de compartilhamento, edição de arquivos offline etc.

O One Drive é o serviço de armazenamento em nuvem da Microsoft. O serviço é gratuito para usar a partir da adesão do usuário ao pacote Office, oferecem editores de textos, planilhas, apresentações e acesso a projetos colaborativos pela internet.

O Dropbox é uma outra opção para armazenar conteúdos na nuvem gratuitamente. Com apenas um registro, o usuário tem acesso a uma conta gratuita e

já pode começar a guardar seus arquivos, dados e informações em um servidor online sem custos extras.

12. Conclusão

Ao longo deste artigo, foi confirmado a necessidade do cumprimento da Lei de Proteção de Dados. Ela facilita o controle dos dados tratados, impõe deveres e responsabilidades aos agentes de tratamento e proporciona segurança para que as informações circulem. Visa-se antecipar os riscos de violação à privacidade, como também evitar tratamentos abusivos de informações e vazamentos de dados e reforça o uso das melhores práticas de segurança da informação. O titular dos dados pessoais se torna apto a exercer seus direitos, a utilizar somente o que tange nos dados pessoais, limitar sua coleta ao minimizo necessário, autorização de revogação do consentimento ou exclusão, a qualquer momento.

As empresas devem ser mais transparentes e conscientes em relação ao uso de dados pessoais, prevenir vazamentos de dados e ameaças que possam vir a comprometer informações, para isso é recomendado o armazenamento em nuvem, tecnologia que permite o gerenciamento e armazenamento físico de dados como serviço, obtendo assim agilidade e acesso aos dados a qualquer momento, em qualquer lugar. A Gestão de Riscos dos ativos na Nuvem permite alinhar a exposição ao risco e a capacidade de gerenciar a tolerância ao risco do proprietário dos dados. Desta forma, caracteriza-se como principal meio de decisão e suporte para proteger a confidencialidade, integridade, e disponibilidade dos ativos de informação na Nuvem.

Muitas pessoas desconfiam e não se sentem seguras com as informações armazenadas em nuvem, porém as empresas fornecedoras da computação investem bastante em soluções avançadas de segurança, capacitação, “antivírus em nuvem”, além de ferramentas capazes de detectar e evitar os mais diversos tipos de ameaças rapidamente. É altamente recomendado a utilização desta tecnologia desde contratações pagas à serviços disponibilizados gratuitamente, pois essa adoção acelera o processo de transformação digital e implementação de requisitos de segurança.

REFERÊNCIAS

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acessado em 21/04/2021

http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acessado em 28/04/2021

Araújo, G. (2020). Os impactos da LGPD para as ações de Segurança da Informação. Disponível em: https://cio.com.br/os-impactos-da-lgpd-para-as-acoes-deseguranca-da-informacao/. Acessado em 28/04/2021

SOUSA, Flávio RC; MOREIRA, Leonardo O.; MACHADO, Javam C. Computação em nuvem: Conceitos, tecnologias, aplicações e desafios. II Escola Regional de

Computação Ceará, Maranhão e Piauí (ERCEMAPI), p. 150-175, 2009. Acessado em 26/04/2021

RUSCHEL, Henrique; ZANOTTO, Mariana Susan; MOTA, W. da C. Computação em nuvem. Pontifícia Universidade Católica do Paraná, Curitiba, Brazil, 2010. Acessado em 15/03/2021

PEDROSA, Paulo HC; NOGUEIRA, Tiago. Computação em nuvem. artigo disponível em http://www. ic.unicamp.br/~ ducatte/mo401/1s2011, v. 2, 2011. Acessado em 20/03/2021

GARCIA, Lara Rocha et al. Lei Geral de Proteção de Dados (LGPD): Guia de implantação. Editora Blucher, 2020. Acessado em 30/04/2021

https://www.trf3.jus.br/seti/seguranca-da-informacao/dicas-da-seguranca-da-informacao/destaques-da-seguranca-da-informacao/codigos-maliciosos-o-que-sao/?sword_list[]=Si&no_cache=1. Acessado em 10/04/2021

https://irisbh.com.br/ataques-hackers-a-orgaos-publicos-e-lgpd-o-que-esperar-do-futuro/ Acessado em 08/04/2021.

DE, LEI GERAL DE PROTEÇÃO. DADOS PESSOAIS (LGPD). 2019.
https://www.techtudo.com.br/listas/2020/11/ataque-hacker-ao-stj-seis-coisas-que-voce-precisa-saber-sobre-o-caso.ghtml - Acessado em 12/04/2021.

https://www.poder360.com.br/justica/stj-restabelece-sistemas-de-informatica-15-dias-depois-de-ataque-hacker/ - Acessado em 30/04/2021.

https://alexandrepontieri.jusbrasil.com.br/artigos/1118681218/lgpd-e-a-experiencia-do-ataque-hacker-ao-portal-do-stj - Acessado em 30/04/2021.

https://www.redhat.com/ptbr/topics/security/cloudsecurity#:~:text=A%20seguran%C3%A7a%20na%20nuvem%2C%20ou,infraestruturas%20envolvidas%20na%20cloud%20computing.&text=Como%20qualquer%20ambiente%20de%20computa%C3%A7%C3%A3o,e%20os%20sistemas%20est%C3%A3o%20seguros - Acessado em 01/05/2021

https://aws.amazon.com/pt/what-is-cloud-storage/ - Acessado em 01/05/2021

https://santodigital.com.br/lgpd-como-nuvem-pode-ser-uma-aliada-na-adequacao-nova-lei/ - Acessado em 01/05/2021