A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS: Um estudo de caso sobre a LGPD na cooperativa de crédito na cidade de Franca-SP.

Ricardo Donizeti da Silva
Graduando em Sistemas de Informação – Uni-FACEF
ricardo.donisilva@gmail.com

Leandro Borges
Mestre em Computação – Uni-FACEF
leandro.borges@facef.br

Resumo
Com o avanço tecnológico que vêm se intensificando cada vez mais, os ataques cibernéticos estão se tornando mais frequentes, desse modo é necessário a implementação de regulamentos (leis) que visam fornecer os usuários mais proteção em relação aos seus dados pessoais. Sendo assim a Lei Geral de Proteção de Dados (LGPD) surgiu para garantir maior segurança das informações pessoais das pessoas físicas. O presente estudo tem por objetivo entender a LGPD, suas aplicações e impactos na cooperativa de crédito. A pesquisa se deu de forma qualitativa, realizada em uma cooperativa de credito da cidade de Franca-SP, onde foi elaborado um questionário direcionado aos gestores da área em relação a implementação da LGPD na cooperativa de crédito. Observou-se que, mesmo com a lei em vigor e com suas penalidades, ainda a cooperativa não está em compliance com a LGPD.

Palavras-chave: LGPD. Segurança de Dados. Cooperativa de crédito.

Abstract
With the technological advancement that intensifies more and more, cybernetics are becoming more frequent, thus it is necessary to implement standards (laws) that aim to provide users with more protection in relation to their personal data, thus being General Law The Protection of Data (LGPD) was created to ensure greater security of personal information of individuals. This study aims to understand the LGPD, its actions and impacts on the credit union (Sicoob). A qualitative research was carried out in a credit union in the city of Franca-SP, where a questionnaire was designed for managers in the area, in relation to the implementation of the LGPD in the credit union. It was observed that even with the law in force with its penalties, the cooperative is not fully in accordance with the LGPD.

Keywords: LGPD. Data Security. Credit cooperative.

1 Introdução

Com o frequente desenvolvimento tecnológico que vem se intensificando principalmente nos últimos anos, se faz necessário a criação de regulamentos (leis), que visam fornecer maior segurança aos indivíduos em relação aos seus dados pessoais. Sendo assim a LGPD foi sancionada em 2018 e entrando em vigor em setembro de 2020, mas a sua penalidade vigorou em 01/08/2021, por esse fato é relevante realizar uma abordagem por meio desse estudo de como a cooperativa de crédito está se adequando a essa exigência, já que atualmente as organizações estão sujeitas as sanções (multa) ao não cumprimento da lei.

O objetivo desse artigo é entender a LGPD e suas aplicações na cooperativa de crédito e seus impactos. Apesar das penalidades da LGPD passar a valer em agosto de 2021 no Brasil como já mencionado, a lei já existia em outros países com o mesmo propósito, mas conhecida por nomenclaturas diferentes.

Foi feito um estudo de caso em uma cooperativa de crédito – em Franca -SP sobre a implementação da LGPD e a mesma já segue à risca todas as leis já existentes sobre tratamentos de dados, mas com a chegada da Lei Geral de Proteção de Dados (LGPD) o processo ficou mais rigoroso e fez a cooperativa repensar em seus processos de coletas de dados, armazenamento e exclusão.

Sobre a segurança da informação, é muito importante estabelecer política de segurança, pois através dela promover diretrizes de apoio e poderá ser alinhado com a regra de negócio e também vale frisar a importância de implementar a norma ISO/IEC 27001 e 27002, pois ajudara a cooperativa estar em compliance com a LGPD e neste artigo também está sendo relatado sobre os princípios para boa gestão de segurança da informação.

Todas as empresas estão sujeitas a ataques cibernéticos e poderá ocorrer externamente e também internamente por usuário maliciosos, porém é possível tomar medidas para evitar a violação através de treinamento dos colaboradores, é preciso ter planejamento para que a organização continue prosseguindo com suas atividades mesmo que ocorra falhas é preciso adotar procedimento de backup. Vale ressaltar que os backups devem ser armazenados fisicamente fora do ambiente empresarial, através de empresas como data center ou até mesmo em cloud. Os dados armazenados precisam ser criptografados e classificados de acordo com LGPD e deveram ficar disponível enquanto estiver sendo utilizado pelo sistema, mesmo com as camadas de rede criptografado, hacker poderá obter volumes de dados através de espionagem e para que isto não aconteça e preciso utilizar o preenchimento de trafego (traffic padding), é importante ressaltar que seja coletado informações somente necessárias.

A cibersegurança também conhecido como, segurança da tecnologia e segurança da informação eletrônica, tem como objetivo proteger de ataques cibernético em dispositivos, como computadores, servidores e dispositivos móveis, pois todos que possuem dados podem se conectar alguma rede e com isto está propício aos ataques de maliciosos.

BEST é metodologia que existem para sustentar de maneira contínua os requisitos da LGPD. Ela engloba pessoas processos e tecnologias e todas as áreas de negócios e também está relacionado com gestão de qualidade. Essa metodologia tem oferecido uma abordagem sustentável e adaptável na implementação do sistema gestão, atendendo holisticamente os requisitos da LGPD, visando o desenvolvimento de sistema relacionado a cibersegurança e proteção de dados. E este princípio visa conscientizar e engajar os colaboradores para autotransformação de seus negócios.

A LGPD tem como finalidade ajudar a desenvolver a economia através da tecnologia, mas sem deixar de proteger os direitos de consumidores, pessoas naturais e como controle BEST e SGCSI podem auxiliar na implementação e também veremos as definição de cada autores que são: titular, controlador, operador encarregado dos dados(DPO) e também veremos os tipos de dados , que são categorizado como dados pessoal que são todas as informações pessoa física e dados sensíveis que são dados que pela sua sensibilidade natural que pode ocasionar discriminação daquele indivíduo. Vale frisar que ao coletar dados é preciso saber a

finalidade e coletar somente o necessário para funcionalidade do sistema, para evitar futuras sanções. Será citado também autoridade nacional de proteção de dados (ANPD) que tem objetivo de verificar e validar a aplicação da LGPD. Este órgão tem a competência para tomar decisões próprias sobre regulação da LGPD.

2. Segurança da Informação

2.1 – **Política de Segurança**

De acordo com Kaspersky (2021), com o avanço da tecnologia também vem aumentando os ataques cibernéticos em todo mundo, principalmente no Brasil. Os principais ataques que estão ocorrendo são da classe HackTool e DangerousObject.Multi.Generic.

De acordo com Demartini (2020), os golpes cibernéticos aumentaram muito em 2020 e a tendência nesse ano é se tornar ainda mais comum, devido às medidas adotadas por causa da pandemia como Home Office e o comércio eletrônico.

Honeynet conhecido como “pote de mel” ou “prisão” é um sistema que é criado com objetivo de ser atacado por hackers, com isso após o sistema ser comprometido tem várias finalidades, sendo umas delas um mecanismo de alerta e também é possível monitorar detalhadamente com precisão o que o invasor gostaria de obter através desta possível invasão, assim o profissional de TI poderá usar essas informações para proteger os dados (COSTA,2002).

É de sumo importância que as organizações tenham gerenciamento de riscos, porque através deste é possível planejar e organizar, assim diminuindo o nível de risco de perda de lucro e principalmente vazamento de dados. Existem vários padrões de gerenciamento de risco e podemos destacar a normativa ISO 27005 que tem como diretrizes auxiliar na implementação para gerenciamento de risco de segurança. Este processo é contínuo em todos os aspectos operacionais, possui colaborador responsável somente para monitoramento destes processos conhecido como *information security officer* -ISO (encarregado de segurança da informação) ou *chief information security officer* – CISO (chefe de segurança da informação). Vale destacar que para implementação do processo é necessário levantar alguns requisitos de segurança da informação que são: avaliação de risco a organização, os requisitos legais e o conjunto de princípios (OLIVEIRA,2010).

É necessário que as organizações tenham Políticas de Segurança da informação, pois através do mesmo promoverá diretrizes de apoio, que deverá ser definido junto com regra de negócio e aprovado pelo conselho administrativo e publicado para todos os colaboradores e fornecedores. É possível publicar de várias formas, uma delas pode ser através de manuais e entregue a todos colaboradores e outra forma seria através da intranet. Vale destacar para implementação da Políticas de segurança da Informação é preciso seguir a norma ISO/IEC 27001 (information Security Management) na qual tem como objetivo de estabelecer normas para segurança da informação e também ISO/IEC 27002 parte I e II que possui códigos de boa prática para controles de segurança da informação (OLIVEIRA,2010).

Podemos também destacar a importância de compreender os requisitos de segurança da informação, pois é necessário estabelecer políticas e objetivos na implementação e operar controles para gerenciamento de riscos. É de sumo importância monitorar e revisar as políticas de segurança para mensurar a eficácia e

desempenho do mesmo. Alcançar, definir e manter a melhoria contínua para que isto se torne essencial para a sobrevivência da organização. Tanto como no setor público ou privado a segurança da informação tem seu objetivo de evitar ou reduzir riscos de ameaças ou fraudes espionagem e sabotagem (OLIVEIRA,2010).

2.2 Princípios Segurança da informação

Entre vários princípios para uma boa gestão de segurança da informação, podemos destacar como principais confidencialidade e exclusividade que se refere ao nível de segurança necessário para assegurar sigilo total das informações coletadas, podemos ressaltar que é de extrema importância coletar somente dados essenciais para o funcionamento do sistema. É imprescindível que o armazenamento desses dados seja de modo criptografado e classificado de acordo com a norma LGPD. E também é muito importante ter controle de acesso às informações e assegurar que os dados ficara somente disponíveis enquanto estiverem sendo utilizados pelo sistema (OLIVEIRA,2010).

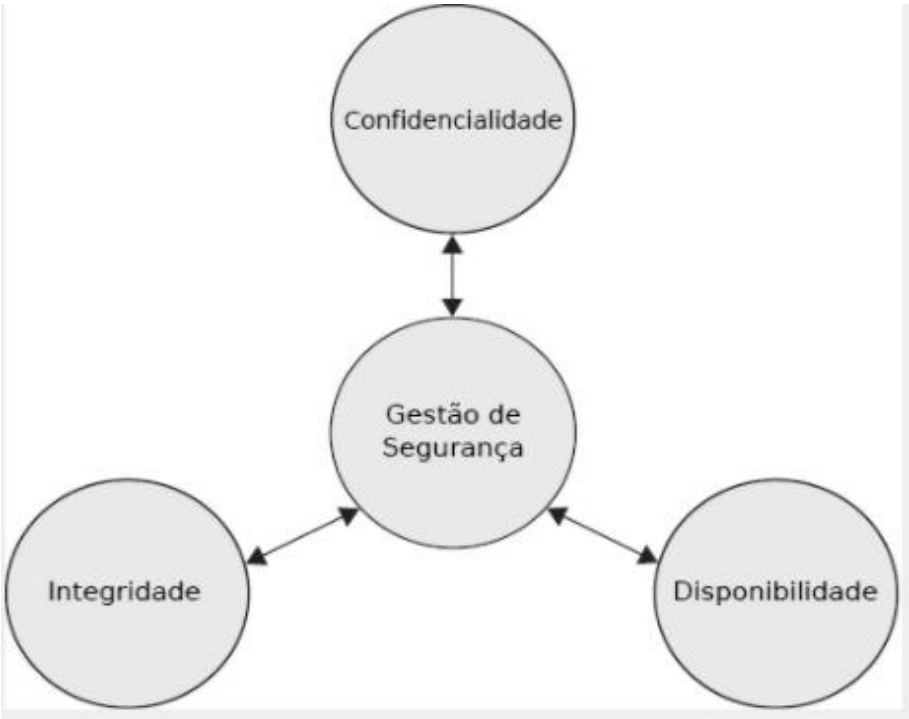
Mesmo com camadas de rede criptografadas é possível que hacker consiga atacar e obter volumes de dados através de espionar a entrada e saída de dados, no entanto para que isto não aconteça é recomendado que haja preenchimento de tráfego (*traffic padding*), pois será impossível que hacker identifique entre fluxo de dados verdadeiro ou do que foram preenchidos (OLIVEIRA,2010).

Outro princípio importante é a integridade dos dados, que consiste que os dados após o armazenamento sejam intactos, a qualquer modificação tanto por erro de usuário ou por ataques de hacker ou até mesmo por problemas de controle de disco que também é considerado violação de integridade. Por sua vez, se o sistema é afetado, poderá afetar negativamente a integridade dos dados substituídos ou apagados. Estes ataques podem acontecer externamente ou até mesmo internamente por usuários maliciosos, porém é possível tomar medidas para evitar a violação através de treinamento de colaboradores que irão trabalhar com esses dados (OLIVEIRA,2010).

A disponibilidade está relacionada à disposição das informações quando solicitada e para que estas informações estejam sempre disponíveis é preciso tomar medidas para que não ocorra violação de disponibilidade, por isso é necessário que haja planejamento para que a organização continue prosseguindo com suas atividades mesmo que ocorram falhas. Por tanto é necessário que adote procedimento de backup, caso ocorra alguma falha sistêmica ou até mesmo por ataques de hacker por negação de serviço (*Denial-of-service*). Com backup é possível substituir rapidamente os arquivos danificados, ou até mesmo servidores comprometidos. Outra medida para uma boa gestão de segurança, seria o monitoramento do tráfego da rede e atividade da máquina através de políticas de segurança estabelecidas nos firewalls e antivírus. Vale ressaltar que os backup devem ser armazenados fisicamente fora do ambiente empresarial, através de empresas como data center ou até mesmo em cloud. Existem algumas organizações que possuem particularidades em casos de agências bancárias por via regra é proibido armazenar dados sigilosos em outros data center fora do Brasil (OLIVEIRA,2010).

Podemos ressaltar que cada organização possui regras de negócios distintas e com isto o nível de segurança e mecanismo de proteção também terão suas particularidades. Segue abaixo ilustração CID (OLIVEIRA,2010).

Figura 01- Gestão de segurança



Fonte: Garcia,2020

2.3 Cibersegurança

Cibersegurança também é conhecido como segurança da tecnologia e segurança da informação eletrônica, tem como objetivo proteger de ataques cibernético em dispositivos, como computadores, servidores e dispositivos móveis, pois todos possuem dados podem se conectar alguma rede e com isto está propício aos ataques de maliciosos (Kaspersky,2021).

De acordo com Kaspersky,(2021) a cibersegurança pode ser dividida em algumas categorias como segurança de rede, segurança de aplicativo, segurança de informações, estão relacionados em proteger dados de possíveis ataques de invasores oportunistas, vale ressaltar que nunca instale aplicativos duvidosos, pois a integridade dos dados pode ser comprometido, podendo haver vazamento de dados. Outra categoria que foi citada pelo site Kaspersky, (2021) é a segurança operacional que se trata das permissões de usuários na rede em tratamento de dados. A educação do usuário final é fator de extrema importância, pois o usuário pode introduzir vírus acidentalmente em servidores, computadores, dispositivos móveis através de arquivos ou links enviados por e-mail ou até por periférico de entrada/saída como unidade flash USB, ou unidade disco entre outros. Recuperação de desastre e continuidade dos negócios também é categoria que está relacionada em incidente sobre cibersegurança que pode causar perda de dados ou de operações, sua definição é que as organizações tenham capacidade de restaurar informações e com isto preservando a continuidade do negócio.

De uma forma geral, vem crescendo exponencial a violação de dados a cada ano. De acordo com Kaspersky (2021) foram 7,9 bilhões de registro violados em

2019, em comparação com mesmo período no ano anterior, esse número dobrou. Entidades públicas varejista e serviços médicos, são o que mais sofrem ataques cibernéticos, pois para mal-intencionado estes segmentos são os mais atrativos, pois é possível coletar dados financeiros e também hospitalar. A International Data Corporation com crescimento de ataques virtuais prevê que haverá gasto de 133, 7 bilhões dólares até 2022 em soluções de cibersegurança. Os governantes, tem orientado as organizações a implementar boas práticas de segurança para combater a ameaça virtual. A cibersegurança combate crimes virtuais, ataques cibernéticos e terrorismo cibernético. Em alguns países criou regulamentos e orientações ou até mesmo agências como no caso dos EUA, National Institute of Standards and Technology(NIST) para eliminar propagação de códigos maliciosos de forma precoce monitorando em tempo real.

3. Metodologia BEST

3.1 O que é metodologia BEST

De acordo com Garcia (2020) a metodologia BEST (Business Engaged Security Transformation) existe para sustentar de maneira contínua os requisitos da LGPD, é sistema de gestão que engloba pessoas, processos e tecnologias e todas as áreas de negócio. E também está relacionado com gestão de qualidade que foi desenvolvido na década de 90 e, desde então, tem sido para quem implementou nas empresas um caminho de sucesso.

Essa metodologia tem oferecido uma abordagem sustentável e adaptável na implementação do sistema gestão, atendendo holisticamente os requisitos da LGPD. Foi criado pela Fundação Vanzolini, visando o desenvolvimento de sistema relacionado a cibersegurança e proteção de dados. E tem como diferencial conscientizar e engajar os colaboradores para autotransformação de seus negócios e, de acordo com autor, são: processos e sistemas em atendimento aos requisitos de garantia da integridade, disponibilidade, sigilo e privacidade das informações transmitidas, processadas e armazenadas pela empresa. Vale frisar que cada colaborador da área de tecnologia da informação voltado para área de infra e segurança de dados, dentro da empresa ou consultores externos, é de extrema importância que sejam vigilantes a respeito de tornar cada vez mais o sistema de informação mais seguro, resiliente e confiável, criando restrições e soluções e implementado de acordo com ambiente da empresa.

3.2 – Princípios da metodologia

A metodologia BEST possui elementos chaves como Mindset que tem como objetivo transformar a mentalidade dos colaboradores, fazendo que os mesmos entendam a importância das obrigações de cibersegurança e, com isto, acabam fazendo parte da cultura organizacional. Responsabilidade e engajamento dos colaboradores é outro princípio, é relevante que cada indivíduo da organização execute as atividade dos negócio com responsabilidade, visando os valores gerado para seus clientes internos e externos. É de suma importância que os colaboradores estejam engajados no processo das obrigações cibersegurança e, isto será fator de sucesso nas atividades de negócio.

Existem outros elementos chaves como agente de transformação que tem como finalidade conscientizar e mudar mentalidade dos colaboradores de forma que obtenha boa relação de custo e benefício, é preciso de agente de transformação para superar as dificuldades pessoais em relação com a tecnologia nos processos.

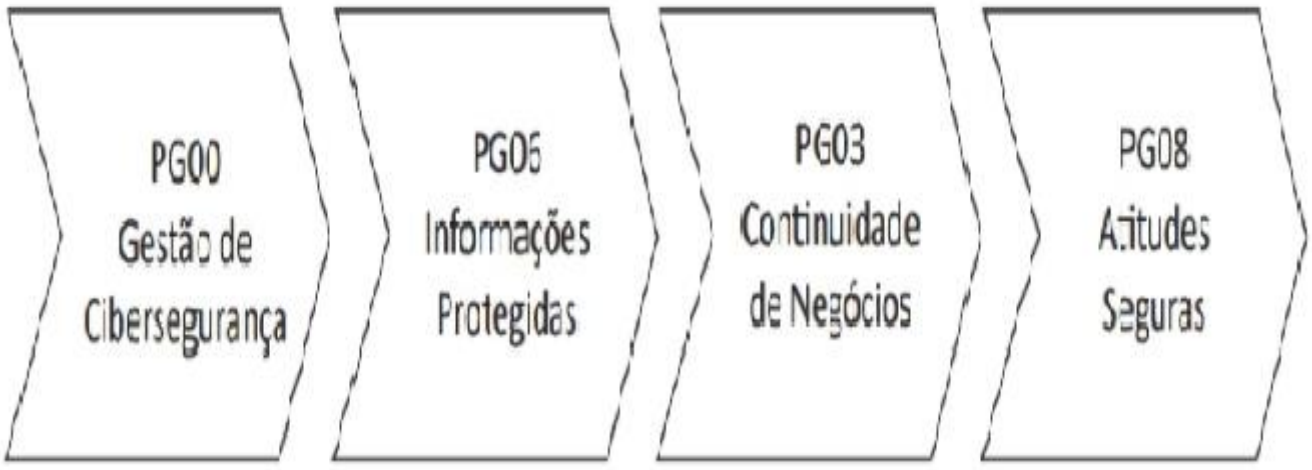
Outros princípios é velocidade que está relacionado com alinhamento entre o ritmo e objetivo para que possa reduzir possíveis conflitos com clientes e com isto é necessário utilizar metodologia adequada que neste caso seria método ágeis por ser mais flexíveis e com isto melhor se adaptam entre cibersegurança e atividade de negócio. É preciso ter alinhamento estratégico com os colaboradores entre nível de competência e avaliação das atividades do negócio, este alinhamento também faz parte do elemento da metodologia Best. É de extrema importância que organizações trabalhem com melhoria contínua nos processos, visando melhoria nos procedimentos e sistemas no qual todos os colaboradores são responsáveis por identificar oportunidades de melhorias em eventos cibersegurança.

4. LGPD

4.1 – Implantação da LGPD

Neste capítulo serão citados somente os controles do BEST relacionado com a LGPD que são PG 00- Programa de Gestão de Cibersegurança e Segurança da Informação, PG03 – Programa de Continuidade de Negócios, PG 06 – Programa de Informações Protegidas, PG 08 – Programa de Atitudes Seguras. A ordem de implementação começa pelo PG 00, mesmo não se relacionando diretamente com LGPD, no entanto é necessário na implementação do mesmo, pois através dela haverá consistência e acompanhamento dos princípios e também atenderá aos requisitos previstos no art.50. Segue abaixo a ilustração de ordem de implementação (Garcia, 2020).

Figura 02 - Programa de Gestão



Fonte: Garcia,2020

4.2 PG 00 – Gestão de Cibersegurança

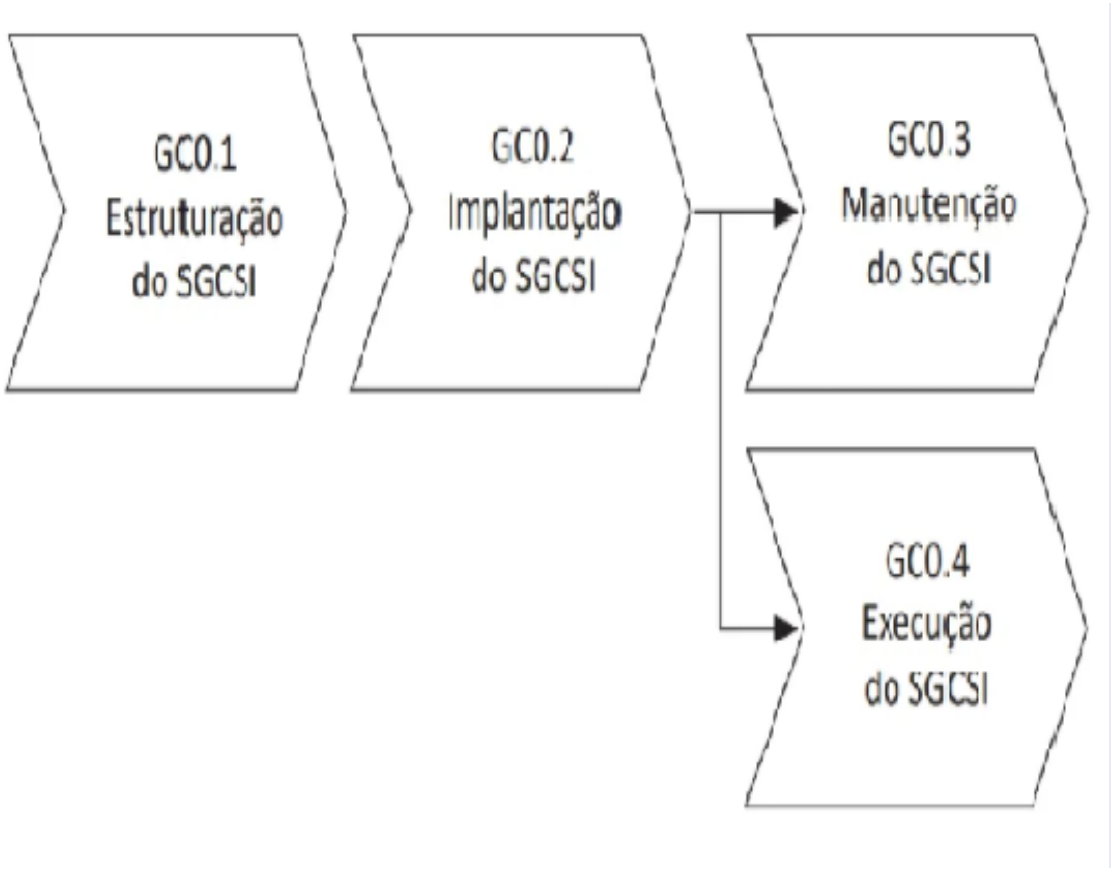
Considera-se que a implementação dos requisitos da LGPD, requer a instalação de um sistema de gestão adequado ao propósito da lei e a um estágio organizacional e econômico de cada organização para isto poderá utilizar o sistema de gestão de segurança de rede e da informação (SGCSI). No art. 50 define que o controlador e o operador podem elaborar regras de boas práticas de governança individuais ou coletivas. A instalação do SGCSI é a fonte de apoio aos requisitos (GARCIA, 2020).

De acordo com Garcia(2020):

> Conforme o artigo 50 a implementação de governança de proteção de dados exige alguns requisitos: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de mo-nitoramento contínuo e avaliações periódica.

Os requisitos acima estão focando em atender integralmente a implementação do PG 00 – Programa Gestão de Cibersegurança e Segurança da Informação e o mesmo está dividido em quatro grupos de controles, GC 0.1. Estrutura do SGCSI, GC0.2. Implantação do SGCSI, GC0.3. Manutenção do SGCI, GC 0.4. Execução do SGCSI.

Figura 03 – Gestão Cibersegurança



Fonte: Garcia,2020

Observe que as medidas de controle relacionadas à estruturação, implantação, manutenção e execução do SGCSI são separadas para melhor entendimento do processo. Compreensivelmente, a estruturação inicial é necessária antes da implementação, pois a implementação deve ser realizada em fases, respeitando o modelo de negócios da organização. Deverá ter como prioridade a implementação do LGPD do que rever a segurança da rede. No entanto é necessário a manutenção do SGCSI, porque as organizações constantemente estão se renovando com novo modelo de negócios, estruturas e com isto novas práticas também precisam ser implementadas. No entanto, para processos ou áreas onde o SGCSI foi realizado, o mesmo deve ser implementado de acordo com os regulamentos.

4.3 PG 06 – Informações protegidas

De acordo com GARCIA (2020), o gerenciamento de requisitos para informações protegidas visa definir e manter os requisitos aplicáveis a demais manuseio do PG06 e também está inserido no método BEST. O Programa de Informação Protegidas (PG 06) tem como objetivo proteger informações sensíveis no contexto de armazenamento e processamento e contém os seguintes grupos de controles a seguir:

> GC6.1. – Gerenciar requisitos para Informações Protegidas: trata do estabelecimento do modelo de classificação de informações, da

> caracterização dos tratamentos e da arquitetura técnica, bem como do estabelecimento dos papéis de Controlador, Operador e Encarregado no contexto LGPD. GC6.2. – Captura da Informação: aborda os aspectos de captação de dados com a respectiva autorização do Titular. GC6.3. - Avaliação da Informação: trata da aplicação do modelo de classificação. GC6.4. – Acesso à Informação: trata dos controles e do registro de acesso às informações sensíveis. GC6.5. – Remoção da Informação: trata da exclusão de informações nas condições determinadas pela LGPD. GC6.6. – Tratamento Ético: determina quando o processamento pode ser considerado ético e, portanto, legítimo, além de abordar as hipóteses de tratamento previstas na LGPD. GC6.7. – Acesso às mídias de armazenamento: trata do acesso físico às informações sensíveis. GC6.8. – Auditoria de Segurança e Privacidade: trata das atividades de auditoria determinadas pela LGPD. GC6.9. – Atendimento a Solicitações: trata do atendimento de solicitações pelos diversos atores definidos na LGPD. GC6.10. – Comunicação de Incidentes: trata dos requisitos de comunicação à Autoridade Nacional de Proteção de Dados (ANPD). (GARCIA,2020)

4.3.1 – Autores da LGPD

A LGPD, entrou em vigor na data 19/09/2020 e tem a finalidade de proteger os dados pessoais com o “objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural” (LGPD, art. 1). Assim, no que diz respeito à definição da classificação das informações, os dados pessoais precisam ser separados das demais informações e protegidos.

A LGPD quer ajudar a desenvolver a economia através da tecnologia, mas sem deixar de proteger os direitos dos consumidores, pessoas naturais. Visa proteger dados pessoais, que são todas as informações de pessoa física, que seja identificado ou que é identificável, ou seja que possa identificar ou que identifique uma pessoa natural, quando falamos de dados pessoais, normalmente pensamos óbvio que é nome, CPF, identidade, só que é muito mais além disso, qualquer dado que possa de alguma forma identificar é considerado dado pessoal. Podemos usar como exemplo uma figura de mosaico, nós temos várias informações separadas, mas juntas forma um objeto. E não é diferente com os dados pessoais, mesmo não tendo nome ou identidade, juntando os dados que estão separadas é possível identificar uma pessoa então podemos dizer que esses dados são pessoais.

Estamos a todo momento distribuídos dados online que pode ser através de e-commerce ou por aplicativo, principalmente aplicativo de banco, além de ter informações pessoais também tem informações bancárias, ou até offline que pode ser através de uma consulta médica, ou na portaria de um prédio onde é passado identidade. Existe um ditado que diz, quando você não paga por usar determinada ferramenta, você se torna a mercadoria, pois existem empresa coleta os dados e usa só para uma determinada finalidade, outras coletam os dados e compartilhavam com terceiros, podem citar por exemplo os anúncios ou até mesmo ligações cuja empresa onde jamais tivemos contato. Isto ocorre devido a transferência de dados de uma organização para outra e este é um dos motivos que foi criado a LGPD, que obriga as organizações coletar somente os dados necessários para funcionamento do sistema e também estabelece a coleta e o armazenamento, tratamento de dados. Caso a empresa não esteja adequada estará sujeita a sanções que estão previstas na LGPD, como multa que poderá chegar a cinquenta milhões de reais. As empresas que se adequarem de modo acelerado terão vantagem competitiva no mercado.

Ao coletar dados é preciso saber a finalidade, que no caso o porquê estou coletando essas informações e a necessidade desses dados, é realmente necessário para essa funcionalidade, é preciso transparência junto ao cliente explicando, o porquê? o pra que? como? e com quem esses dados serão compartilhados. Só coleta os dados de fato necessários e só usa os dados para finalidade que foi coletado.

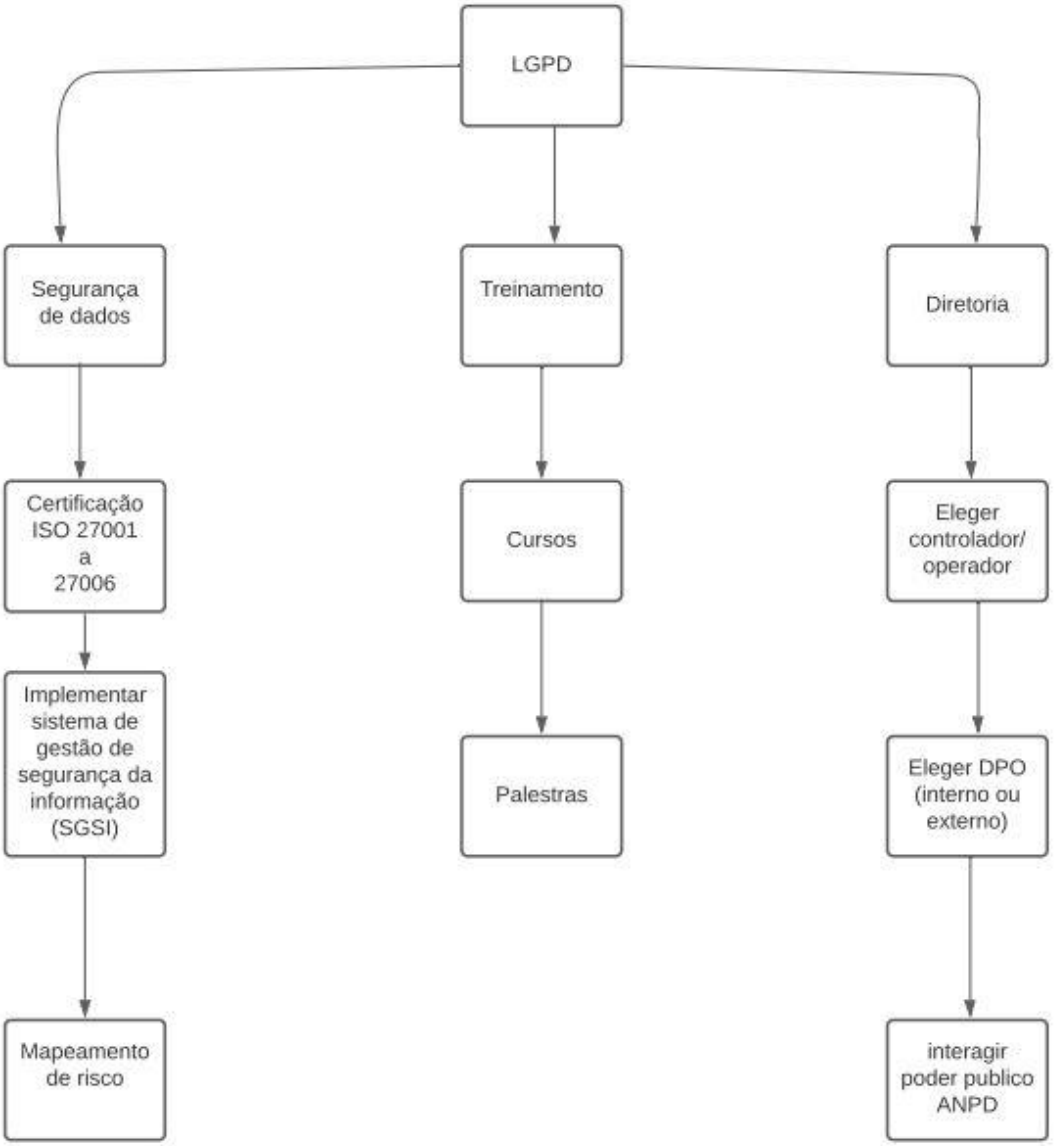
Existe também dados pessoais sensíveis, que são dados que pela sua sensibilidade natural que pode ocasionar discriminação daquele indivíduo, podemos citar como exemplo a religião, orientação sexual, orientação política, raça, tudo que pode levar algum a tipo de preconceito atrás da coleta de dados. É preciso ter atenção também, porque alguns dados originalmente não seriam dados sensível, mas em determinado contexto ele pode ser dados sensível, podemos citar como exemplo dado de geolocalização, por si próprio é dado pessoal, mas não sensíveis, pois identifica o indivíduo mas esses dados não discrimina, mas se sua geolocalização indicar que frequenta uma determinada igreja por exemplo, então se torna dados pessoais sensíveis. Do mesmo modo acontece com dados relacionados a informações médicas, por exemplo tipo sanguíneo ou doença hereditária, informações de funcionário, que no caso seria holerite, e também biometria, reconhecimento facial também é considerado dados sensíveis, tudo que é imutável é considerado dados sensíveis. Só não faz parte dados pessoais, de acordo com a LGPD, redes sociais e mídia impressa que são informações publicadas.

Dentro da LGPD existem quatro autores que são: titular, controlador e operador encarregado. O titular é a parte mais envolvida no tratamento, afinal é a pessoa física a quem se referem os dados pessoais ele é o proprietário dos dados, o mesmo pode solicitar remoção junto ao controlador e o operador, que é o agente de tratamento. O controlador que toma as decisões referentes ao tratamento de dados pessoais e o operador e que realiza o tratamento de dados pessoais em nome do controlador, é muito importante saber definição por conta da responsabilidade dos agentes de tratamento da LGPD, determina que o controlador o operador se causar algum dano será obrigado repará-lo. Operador responde solidariamente junto com o controlador quando descumprirem, ou quando não tiver seguido as instruções do controlador, já o controlador estiver diretamente envolvido e causarem danos aos titulares serão responsáveis, assim caso o operador atuem em conformidade com lei e atenda rigorosamente às exigência do controlador ele não será responsabilizado por eventuais danos causados pelo controlador.

Data Protection Officer (DPO) no conceito é a pessoa indicada pelo controlador e o operador, para atuar como canal comunicação entre o controlador e os titulares dos dados e a ANPD, o Encarregado pode ser pessoa física ou juridica. O DPO que será responsável pelo atendimento dos pedidos dos titulares e por receber comunicação da ANPD e orientar os colaboradores da organização a respeito de boas práticas a serem tomadas em relação a proteção de dados pessoais (GARCIA,2020).

Para melhor entendimento do processo foi desenvolvida estrutura analítica do projeto (EAP), Para auxiliar a implementação da LGPD.

Figura 04 – Estrutura Analítica do Projeto



Fonte: do Autor

4.3.2 – ANPD

Autoridade nacional de proteção de dados (ANPD) é órgão federal que tem como objetivo verificar e validar a aplicação da LGPD em relação a proteção de dados. Essa autoridade tem competência para tomar decisões próprias sobre regulação da LGPD no Brasil, inclusive aplicando sanções às empresas que não cumprirem a legislação. ANPD é composta por conselho diretor, conselho nacional, corregedoria, ouvidoria, assessoria jurídica própria, e unidade administrativas. A LGPD determinou autoridade nacional de proteção de dados vinte quatros competências, mas nesse artigo citarei apenas zelar pela proteção dos dados de acordo com lei e fiscalizar a aplicação da LGPD no Brasil inclusive aplicando sanções para quem descumprir, promover na sociedade o conhecimento da LGPD, pesquisar e se informar sobre como outros países trabalha com a proteção de dados, editar

regulamentos e procedimentos para ser utilizado por todos aqueles que eventualmente tratem os dados e deliberar sobre a aplicação da LGPD, sempre na esfera administrativa e por fim podemos citar com relevância que é implementar um fale conosco onde poderão ter acesso autoridade nacional de proteção de dados (ANPD) para que a população posso fazer reivindicações. A ANPD é necessária, pois não adiantaria criar várias regras se não tiver nenhum órgão para fiscalizar e aplicasse sanções (GARCIA,2020).

Podemos citar o vazamento de atestado médico através do RH da empresa, cujo o funcionário era portador de HIV e esse vazamento ocorreu devido compartilhamento de impressora com outros setores, pois outro funcionário teve acesso à informação. Por esse e outro exemplo podemos ter noção da importância da implementação da LGPD (EJUR, 2020).

5 – Estudo de Caso

Foi feito estudo de caso do segmento de cooperativa de crédito, que atua no processo de atendimento ao cliente realizando concessão de crédito, comercialização de produtos como consórcio, seguro, máquinas de cartão. Os dados coletados são: Nome, endereço, e-mail, CPF, RG, Titulo de Eleitor, Telefone(s), Profissão, Sexo, Data de Nascimento, estado Civil, Grau de Instrução, Nacionalidade, Dados do Cônjuge, Dependentes, estado civil, Naturalidade, Cônjuge, Regime de casamento, Filiação, Conta bancária, Renda, Assinatura, Foto, Matrícula e Função. Esses dados são coletados através de formulários, telefone e-mail, Whatsapp e são armazenados através de planilhas, e-mail, contratos e arquivos diversos em servidores. E os dados são coletados para atender diversas finalidades, que variam desde o cadastro de colaboradores no sistema de controle de ponto e folha de pagamento, à abertura de conta, análises de crédito, operações de pagamento para clientes e consórcios, na cooperativa também é tratado dados sensíveis. Segundo o gestor da área de tecnologia, atualmente ainda não existe uma política definida prevendo o período de retenção de dados, será definido pela central na próxima auditoria, mas o descarte de documentos impressos é feito com a utilização de fragmentadora, estes dados somente os colaboradores tem acesso dentro das suas respectivas áreas de atuação, é feito o controle através de alçadas que são grupos de acessos.

Os direitos dos titulares são assegurados pelo artigo 17 da LGPD e por questão de segurança da não armazena dados pessoais em servidores fora do Brasil. A cooperativa já utiliza recursos de segurança de perímetro e de endpoint como antivírus e firewall como citado no capitulo 4.3.1 (Autores da LGPD). Foi contratado para implementação da LGPD consultoria especializada de mapeamento dos dados pessoais, sistemas e processos utilizados pela empresa, bem como o levantamento das bases legais de uso dos dados de acordo com a Lei. Ocorrerá também elaboração de auditorias internas e externas que será realizado pela anualmente e por empresas especializadas e também será necessário a implementação da ISO 27002 citado no capitulo 2 (Segurança da Informação).

O controlador e o operador devem preparar um contrato por escrito, garantido a confidencialidade dos dados, listando os objetivos e os métodos de processamento do modo definindo pelo controlador e especificando que o operador conduzira o processamento unicamente conforme as instruções do controlador. As duas partes devem assinar este contrato.

Para que as cooperativas mantenham os dados e sigam com a confiança dos clientes e cooperados elas terão que demonstrar transparência ao se comunicar abertamente sobre quais dados coletam, para quais finalidades, quem é o seu processador de dados e assim por diante citado no capitulo 4 (ANPD) é preciso mais do que nunca ter cuidado com o tratamento de dados das pessoas, pode ser cooperado, funcionário, cliente, fornecedor. Com isso a LGPD ajudara criando rotinas de prevenção e solução de problemas que envolvem privacidade e proteção de dados e também ajudara na atualização de políticas de conduta interna que será responsabilidade do setor controles internos, é provável que central irá disponibilizara treinamentos para todos os colaboradores, pois com isto garantira vantagem competitiva com outras instituição financeiro.

O titular ao concede os dados a cooperativa, o controlador ao verificar e constar algum problema será encaminhado ao encarregado, para que ele faça cumprir o que está na lei junto com ANPD conforme o capitulo 4.3.2 (ANPD) e esse tratamento pode ocorrer dentro da cooperativa pelo setor controle interno, ou senão pela central. Caso o cooperado queira saber o que a cooperativa tem de posse de informação a cooperativa é obrigado atender a solicitação encaminhado para o encarregado (DPO) e o mesmo irá conduzir o processo inteiro para que haja êxito na resposta ao titular e, com isto, garantido que não haja sanções referente a LGPD.

A cooperativa também trabalha com dados peseudomização que são dados pessoais que não podem mais ser atribuído a um titular de dados especifico sem o uso de informação adicionais, mas é um processo reversível então é considerado dado pessoal. E também anomização são dados pessoais que não podem mais ser atribuídos a nenhum titular de dados especifico. Não é reversível então não é considerado dados pessoais, é possível ser utilizado, mas de forma estatística então não dá para saber quem é o titular.

Existem dez hipóteses permitidas para tratamento de dados, mas para cooperativa as hipóteses mais importantes é execução de contrato, pois o simples ato de contratar já traz sem si a vontade de materializar o registro dos dados das partes no instrumento contratual, para o conhecimento recíproco, pelo menos. E se objeto do contrato for o tratamento de dados do titular, ou tiver esse tratamento como consequência do objeto, a evidente manifestação de vontade que existe se materializa neste instrumento particular válido, firmado entre duas pessoas e é base legal para o tratamento de dados pessoais.

Outras hipóteses é exercício regular de direitos, que confere legitimidade ao uso que os agentes de tratamento façam dos dados tratados para atuação em defesa de seus interesses perante autoridades em processos administrativos ou jurídicas. Outra hipótese proteção da vida do titular ou de terceiros, a privacidade de uma pessoa jamais será considerada um bem maior que vida humana.

Por essa razão, se alguém informa seus dados e circunstancias de acidente, não estava havendo violação de dados. E temos também interesse legitimo que está na base legal dá suporte ao tratamento executando com legitimidade de interesse do agente de tratamento do titular ou de terceiros. A prestação de um serviço que dependa do tratamento de dados torna legitimo ao agente de tratamento dos dados pessoais. Mas a legitimidade desse interesse só prospera se ele se faz coerente com a legitimidade expectativa do titular ou de terceiro em relação a finalidade e aos modos de tratamento. O serviço de Helpdesk depende dos dados do titular para lhe prestar atendimento e facilitar futuras demandas. O uso desses dados

para comercializar cadastro a terceiros viola a legitima expectativa do titular. Outra hipótese importante para cooperativa é proteção ao crédito é escudado por esta base legal. As pendencias obrigacionais, inadimplências e a má-conduta de pessoas naturais e jurídicas na praça são circunstancias lesivas a toda a cadeira creditícia e contrarias aos interesses da sociedade como um todo.

6. Conclusão

O presente trabalho objetivou realizar uma abordagem da implementação da LGPD, realizando um estudo dos seus principais pontos e por fim, foi realizado um estudo de caso na cooperativa de crédito, onde mesmo já seguindo à risca todas as leis existentes sobre o tratamentos de dados, com a chegada da LGPD o processo ficou mais rigoroso , fazendo com que a cooperativa repensasse em seus processos de coletas de dados, armazenamento e exclusão, para que assim a cooperativa consiga maior competitividade no mercado. Chegamos ao resultado que a cooperativa de crédito, ainda se encontra na fase de implementação da lei. Foi feito levantamento de requisito sistêmicos e processos, mas ainda falta a fase dois que será auditado pela central, mesmo já vigorando as sanções (penalidades) a partir de 01/08/2021, a cooperativa não está totalmente em compliance com Lei e assim será necessário a implantação da ISO 27002.

Referências

Kaspersky. Ciberameaça Mapa em tempo real. 2021. Disponível em https://cybermap.kaspersky.com/pt/stats. Último acesso 16 de março de 2021.

Demartini, Felipe. Especialista avisa: ataques cibernéticos serão ainda mais comuns em 2021. 2020. Disponível em https://canaltech.com.br/seguranca/especialista-avisa-ataques-ciberneticos-serao-ainda-mais-comuns-em-2021-176497/. Último acesso 16 de março de 2021.

Kaspersky. Cibersegurança. 2021. Disponível em https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security. Ultimo acesso 12 de setembro de 2021.

Costa, Giselia do Carmo. Conheça o seu inimigo, o projeto honeynet. São Paulo: Pearson Education. 1ª. Edição. 2002.

Oliveira, Sergio Martins. Fundamentos de Segurança da Informação. Rio de Janeiro: SBNigri Artes e Textos LTDA. 3ª. Edição. 2010.

Garcia, Lara Rocha. Lei Geral de Proteção de Dados (LGPD): Guia de implantação.

Secretaria-Geral. Presidênciada Republica. Disponível em http:// www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#art65.. . Último acesso 29 de novembro de 2021.