Universidade de Brasília

Departamento de Engenharia Elétrica

Curso de Engenharia de Redes de Comunicação

LGPD na área de Segurança de Redes: Uma análise na Infraestrutura SOC

Trabalho de Conclusão de Curso de Graduação

por

Alessandro Florencio Dias Junior e

Jorge Roberto Silveira Filho

Orientador: Prof. Georges Daniel Amvame Nze

Brasília, Junho / 2022

Alessandro Florencio Dias Junior e

Jorge Roberto Silveira Filho

LGPD na área de Segurança de Redes: Uma análise na Infraestrutura SOC

Projeto Final de Graduação apresentado ao Curso de Engenharia de Redes de Comunicação, como requisito parcial para a obtenção do Título de Bacharel em Engenharia de Redes de Comunicação, Universidade de Brasília.

Orientador: Prof. Georges Daniel Amvame Nze

Brasília

2022

Agradecimentos

Primeiramente gostariamos de agradecer as nossas famílias, que em todo curso nos apoiaram e nos incentivaram a chegar até aqui, sem vocês isso não seria possível.

A todos os professores que fizeram parte da nossa formação, o nosso muito obrigado. Em especial gostariamos de destacar nosso orientador Professor Georges Daniel, que nos apoiou nessa pesquisa desde o início e sempre nos ajudou a dar o nosso melhor.

Aos colegas que participaram da nossa jornada durante o curso, sabemos que não foi fácil.

Finalmente, gostariamos de agradecer a Deus por tudo.

Todos os momentos estarão gravados em nossa memória.

Mesmo desacreditado e ignorado por todos, não posso desistir, pois para mim, vencer é nunca desistir.

Albert Einstein

RESUMO

Com o advento da globalização, o acesso a Internet se tornou mais popularizado, gerando maior fluxo de troca de informações entre usuários. Com isso, houve a necessidade de elaboração de novas políticas para garantir a segurança e privacidade de dados pessoais. Em Abril de 2016 os países que fazem parte da União Europeia aprovaram o Regulamento Geral de Proteção de Dados (GDPR), que visa fiscalizar a forma de manuseio das informações entre o titular dos dados pessoais e o controlador, bem como a simplificação da regulação das transações internacionais. Em resposta, o Brasil aprovou a Lei Geral de Proteção de Dados (LGPD) em 2018, com o objetivo de estar de acordo com o regulamento europeu e também possuir sua própria política de proteção de dados.

Apesar de os regulamentos serem rígidos, estudos mostram que ainda há muitos desafios a serem contornados na implementação das diretrizes na área de segurança de redes. A falta de profissionais capacitados, a falta de investimento e a recente aprovação da LGPD têm gerado um atraso no entendimento sobre o que precisa ser realizado nas organizações para que o tratamento e processamento de dados estejam em conformidade com as políticas.

Diante dos pontos citados anteriormente, o estudo em questão traz o uso da unidade SOC como uma possibilidade de solução para esses desafios, pois atua na área de detecção de ameaças e detecção e resposta a incidentes, integrando e facilitando a implementação da lei por parte das empresas. Portanto, o objetivo é obter melhor entendimento do atual cenário da regulamentação de proteção de dados, sendo realizado a análise de arquiteturas de rede com diferentes níveis de segurança no intuito de verificar as vulnerabilidades, os possíveis ataques que podem acontecer, os artigos onde a lei é infrigida e como melhorar a defesa para solução dos problemas apresentados. Como resultado, foi construído uma verificação de nível de segurança, bem como um plano organizacional abrangendo a empresa como um todo, sempre buscando a melhoria e utilizando o ferramental SOC e os conceitos pertinentes a segurança da informação para o cumprimento da LGPD no que diz respeito à proteção dos dados.

Palavras-chave: LGPD, GDPR, SOC, Cibersegurança.

ABSTRACT

Due to advancement of technology, internet access has become more popular, increasing information exchange between users. Because of that, new politics were necessary to guarantee security and privacy of personal data. On 2016 April, the European Union approved the General Data Protection Regulation (GDPR), which the purpose is police data processing between data owner and data controller, as well as simplifying international transactions regulation. In response, Brazil also approved its own personal data regulation, called Lei Geral de Proteção de Dados (LGPD), which main goal is to suit European regulation.

Although the regulations are strict, studies show that there are still many challenges to be overcome in the implementation of the guidelines in the area of network security. The lack of trained professionals, lack of investment and the recent approval of the LGPD have led to a delay in understanding what needs to be done in organizations for the treatment and processing of data to be in compliance with with the policies.

Having these points mentioned above as a parameter, the study in question brings the use of the SOC unit as a possible solution to these challenges, because it operates in the area of threat detection and incident detection and response, integrating and facilitating the implementation of the law by companies. Therefore, the goal is to get a better understanding of the current scenario of data protection regulation, analyzing network architectures with different security levels in order to verify the vulnerabilities, the possible attacks that can happen, the articles where the law is infringed and how to improve the defense to solve the problems presented. As a result, a security level check was built, as well as an organizational plan covering the company as a whole, always seeking improvement and using the SOC tool and the concepts pertinent to information security to comply with the LGPD regarding data protection.

Keywords: LGPD, GDPR, SOC, Cybersecurity

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

GDPR	Regulamento Geral de Proteção de Dados
DPA	Autoridade de Proteção de Dados
STJ	Supremo Tribunal de Justiça
LGPD	Lei Geral de Proteção de Dados
ANPD	Agência Nacional de Proteção de Dados
NSA	Agência de Segurança Nacional
SOC	Centro de operações de segurança
NOC	Centro de operação de rede
TJSP	Tribunal de Justiça de São Paulo
SPC	Serviço de Proteção ao Crédito
IOT	Internet das coisas
IA	Inteligência artificial
IP	Protocolo Internet
TI	Tecnologia da Informação
SSL	Camada de Soquete Seguro
CASB	Corretor de segurança de acesso à nuvem
SIEM	Gerenciamento de Incidentes e Eventos de Segurança
DOS	Ataque de Negação de Serviço
IPS	Sistema de Prevenção de Intrusão
DMZ	Zona Desmilitarizada
PSO	Plano de Segurança Organizacional
ITIL	Biblioteca de Infraestrutura de Tecnologia da Informação
PMBOK	*Project Management Body Of Knowledge*

SUMÁRIO

1 INTRODUÇÃO

1.1 Contextualização

O Centro de Operações de Segurança (SOC, do inglês *Security Operation Center*) é uma unidade centralizada composta por pessoas capacitadas, processos e tecnologias que juntos trabalham na segurança de uma organização por meio de investigação, prevenção e detecção de ameaças cibernéticas [1]. A popularização da internet, acompanhada da digitalização de vários serviços como comércio, transações bancárias e ensino remoto, que antes eram feitos apenas pessoalmente, gerou um aumento na quantidade de tráfego de dados pessoais redes, aumentando as responsabilidades dos SOC e gerando questionamentos sobre como é feita segurança, armazenamento e processamento desses dados. Nesse contexto, o Regulamento Geral de Proteção de Dados (GPDR, do inglês *General Data Protection Regulation*) surge na União Europeia para proteger os direitos e liberdades fundamentais das pessoas singulares e, em particular, o seu direito à proteção de dados pessoais [2].

No Brasil, a regulação da proteção de dados, além do GDPR, teve como influência o Marco Civil da Internet, Lei n° 12.965/2014. Esse dispositivo legal da Internet, apesar de não tratar exclusivamente sobre a proteção de dados pessoais, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria [3]. No Art 3°, ao citar os princípios do uso da internet no Brasil, a lei aborda a privacidade, a proteção de dados pessoais e a responsabilização dos agentes, direitos fundamentais protegidos pela Lei Geral de Proteção de Dados (LGPD), Lei n° 13.709/2018.

Figura 1: Linha do tempo da regulação de proteção de dados no Brasil.

A LGPD, em seu Art 6°, determina, além da observância da boa-fé, que os princípios para o tratamento de dados pessoais devem ter finalidade legítima, específicas e informa-

das ao titular, a garantia de informações claras, precisas e facilmente acessíveis sobre o tratamento dos dados pessoais aos titulares, a utilização de técnicas de segurança para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e cumprimento das normas de proteção de dados [4].

Além de estabelecer obrigações legais para o tratamento de dados pessoais por parte dos responsáveis, a LGPD também prevê penalidades a quem descumpri-las. De acordo com o Art 42°, para assegurar a efetiva indenização ao titular dos dados, o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo [4].

Apesar de a nova lei estar em vigor desde 2020, prevendo a existência de obrigações legais e de penalidades aos que a descumprem, as organizações ainda têm dificuldades para implementar um efetivo sistema de proteção de dados. Devido a essas dificuldades, ciberataques aos dados de grandes empresas e instituições públicas, como Supremo Tribunal de Justiça (STJ), Tesouro Nacional, Ministério da Saúde, JBS e Lojas Renner, causaram grandes prejuízos nos anos de 2020 e 2021 [5]. Esses ataques geram questionamentos a respeito da efetiva implementação da LGPD no Brasil. Qual a diferença entre o panorama de proteção de dados brasileiro e na Europa? Como tornar a implementação LGPD eficiente no Brasil? Diante das dificuldades de cumprimento dos regulamentos, o SOC é uma solução?

1.2 Objetivos Gerais

Devido ao cenário mundial de expansão da tecnologia e a constante troca de dados através da internet, o objetivo do estudo em questão é criar um melhor entendimento sobre o atual panorama das diretrizes que padronizam a forma do tratamento dos dados, como exemplo a GDPR e a LGPD, além de explorar as dificuldades apresentadas na implementação da lei na área de segurança da informação e encontrar soluções que auxiliam na conformidade das políticas. Para isso, pretende-se utilizar o método de revisão bibli-

ográfica, que consiste na pesquisa advinda de outros materiais científicos já elaborados e relacionados com o tema desenvolvido no estudo. Tendo como foco os especialistas na área de segurança da informação e as empresas que buscam estar em cumprimento com o regulamento, na intenção de disseminar soluções para os problemas que serão encontrados. A partir desse entendimento é esperado que as regulamentações sejam compreendidas e os principais pontos de atenção para sua implementação sejam explorados.

1.3 Objetivos Específicos

Analisar o panorama do regulamento Europeu, Brasileiro e da ferramenta SOC. Explorar os principais pontos abordados e como se relacionam. Comparar e propor soluções técnicas para uma melhor implementação de regulação de proteção de dados, utilizando o SOC como principal alternativa. Estudar cenários com diferentes níveis de segurança com intuito de verificar as vulnerabilidades, os possíveis ataques que podem acontecer, os artigos nos quais a lei é infrigida e como melhorar a defesa para solução dos problemas apresentados. Elaborar um Plano de Segurança Organizacional (PSO) capaz de difundir e facilitar a implementação das ideias de segurança da informação contidas na LGPD.

1.4 Estrutura Documental

Para o presente trabalho realizou-se uma revisão bibliográfica, que, de acordo com Gil (2002), trata-se de uma pesquisa desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos [6]. Na busca de artigos optou-se por aqueles publicados no período de Janeiro de 2018 a Janeiro de 2022. O período foi escolhido por coincidir com discussões da elaboração, aprovação e primeiros anos de vigência da LGPD.

A partir dos artigos e reportagens obtidos, a revisão bibliográfica foi desenvolvida por meio de uma análise comparativa entre a situação no exterior e a situação brasileira, abordando o panorama da regulação de proteção de dados no Brasil e na Europa, bem como o panorama geral de SOC. Tendo em vista essa análise, o objetivo principal do estudo é identificar as principais dificuldades da implementação técnica da LGPD no Brasil, em comparação com a implementação europeia, além de apontar possíveis causas e soluções técnicas para essas divergências. O fluxograma da Figura 2 descreve como a

metodologia proposta foi elaborada durante o trabalho.

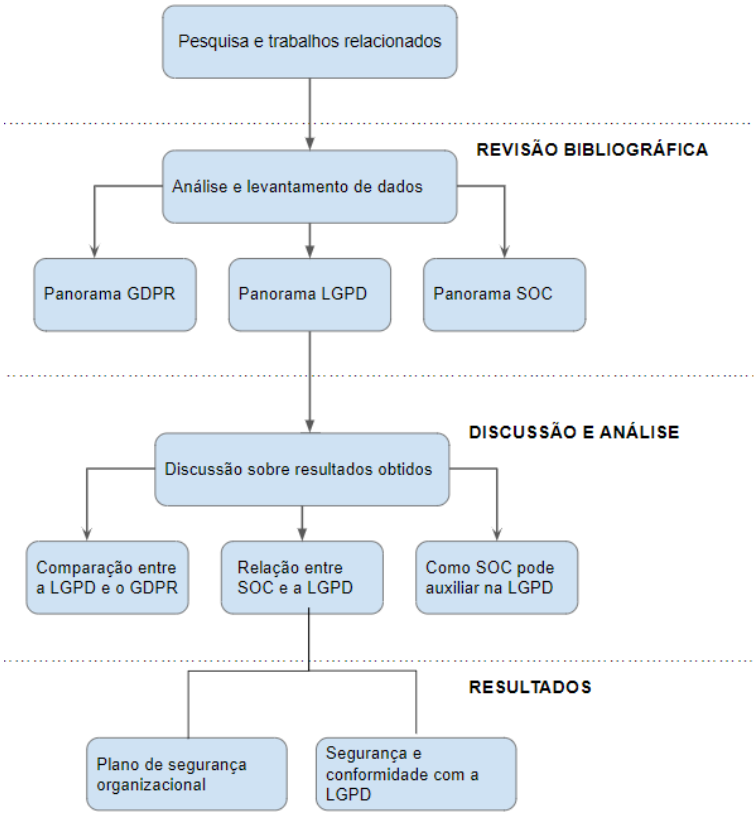

Figura 2: Fluxograma da estrutura documental.

2 REVISÃO BIBLIOGRÁFICA

2.1 Panorama da regulação de proteção de dados na Europa

O direito de privacidade, de acordo com a concepção atual, tem como finalidade estabelecer limites para intromissão na vida privada de um indivíduo e, é caracterizado pela liberdade de autodeterminação informativa, ou seja, é a capacidade do titular em controlar suas informações pessoais [7]. A popularização da internet, acompanhada da prestação de serviços digitais, fez com que o titular perdesse o controle de suas informações pessoais. Em 2013 as revelações do americano Edward Snowden sobre um sistema de vigilância global mantido pelos Estados Unidos, através da Agência de Segurança Nacional (NSA, do inglês *National Security Agency*), geraram debates acerca da violação do direito de privacidade dos indivíduos. Nos documentos divulgados, foi exposto que a NSA realizou acordos clandestinos com empresas do Vale do Silício, para ter acesso aos dados dos consumidores como fotos, e-mails e videoconferências [8]. Nesse contexto foi aprovado na Europa, em Abril de 2016, o Regulamento Geral de Proteção de Dados, que entrou em vigor em Maio de 2018. O GDPR tem como objetivo melhorar o controle e os direitos de privacidade dos indivíduos sobre seus dados pessoais e simplificar a regulação para negócios internacionais. Os principais pontos abordados no GDPR referentes à segurança da informação são apresentados na Tabela 1.

Tabela 1: Princípios do GDPR referentes à segurança da informação.

Artigo	Descrição
Art 4°	São demonstradas as definições de todo escopo que será tratado no regulamento, demonstrando o significado de cada conceito como por exemplo os tipos de dados, o papel do controlador, a autoridade supervisora, o processo, dentre outros.
Art 5°	Neste artigo são informados os princípios relativos ao tratamento de dados pessoais, bem como o procedimento de realização da divulgação elencando os pontos como transparência, justiça, licitude, adequação e relevância.

Art 24°	Corresponde a responsabilidade do controlador, que está relacionada na elaboração de medidas técnicas visando a adequação para assegurar e poder demonstrar que o tratamento seja efetuado em conformidade com o regulamento.
Arts 32°, 35°, 36° e 37°	Todos os artigos estão relacionados à segurança da informação, relacionando medidas de segurança que visam a garantia dos princípios de confidencialidade, disponibilidade e integridade, avaliação de impacto, definição de responsáveis pela operação dos dados e realização de consulta prévia com a autoridade supervisora para análise do que está sendo realizado.
Art 33°	Tem como objetivo definir o prazo de comunicação ao titular e a autoridade quando houver violação dos dados, além de documentar todos os fatos relacionados à invasão.
Arts 40°, 41° e 42°	Todos os artigos estão relacionados com o código de conduta dos quais os controladores devem se guiar para o tratamento dos dados, além do monitoramento desses códigos de conduta pelas autoridades competentes e as certificações que visam demonstrar o cumprimento por parte organizações com os padrões estabelecidos no regulamento.

A partir dos pontos citados, percebe-se que a lei é bem rígida no que condiz as especificações para os responsáveis pelo tratamento dos dados e as medidas a serem tomadas para defesa da organização. É importante acrescentar que o descumprimento da lei pode acarretar em multas. Para monitoramento de tal ação é utilizada a ferramenta *GDPR Enforcement Tracker* [9], que registra, detalha e contabiliza as penalidades aplicadas em decorrência de descumprimentos com os termos da lei. Além de um desafio de privacidade dos dados pessoais, o GDPR também é um desafio de segurança da informação para as organizações e, é necessário entender como o padrão ISO 27001, que trata desse assunto,

pode influenciar na implementação do regulamento.

No artigo *"Implementation of ISO 27001 Standards as GDPR Compliance Facilitator"*, de Lopes, Guarda e Oliveira [10], o objetivo principal do estudo é responder como a norma pode facilitar a implementação da nova lei. Na discussão foram levantados 9 pontos que do padrão ISO 27001 que podem auxiliar na na adequação da organização com o GDPR:

- O GDPR recomenda o uso de certificados, então o uso do padrão ISO 27001 é uma forma de garantir que a organização está gerindo bem os riscos de segurança da informação;
- O padrão 27001 protege não apenas os dados pessoais, mas todos ativos de informação;
- O GDPR prevê que as organizações devem selecionar ferramentas de controle para mitigar os riscos identificados, assim como é previsto no padrão ISO 27001;
- Pessoas, processos e tecnologias. Os três aspectos fundamentais de segurança da informação devem ser levados em consideração ao implementar o GDPR;
- No padrão ISO 27001 é exigido que as organizações possuam um Indivíduo Sênior que seja responsabilizado pelo sistema de gerenciamento de segurança da informação. No GDPR é exigido um responsável pela proteção de dados da organização;
- No padrão 27001 é previsto que as organizações tenham um sistema de avaliação de riscos para identificar ameaças e vulnerabilidades. No GDPR é especificado que as organizações tenham avaliação de riscos para mitigar o impacto dos riscos nos dados pessoais;
- No padrão ISO 27001 é previsto que as organizações tenham uma política de melhoria contínua, de modo que os sistemas de gerência de segurança da informação se adaptem a mudanças;
- Estar em conformidade com a LGPD demanda testes e auditorias regulares, para provar que a segurança adotada é eficiente. Testes e auditorias nos sistemas de gerência de segurança da informação são requisitos para se obter o certificado ISO 27001;

- Certificado da ISO 27001: É uma forma de garantir que a organização implemente medidas adequadas para proteger suas informações.

Apesar de facilitar a implementação do GDPR, o padrão ISO 27001 não contempla todos os pontos da lei, já que consentimento, portabilidade de dados, direito de esquecimento, direito de restrição de processamento, direito de oposição e transferência internacional de dados pessoais são pontos presentes apenas no GDPR. A conclusão dos autores é de que o uso de certificados do padrão ISO 27001 facilita a implementação do GDPR em uma organização, mas não é suficiente para que a mesma esteja em conformidade com a lei.

No artigo *"GDPR impact on Information Security Incident detection and response"* de Andrea Imrichová [11], no qual consiste em realizar uma pesquisa relacionando SOC e a regulação do GDPR, abordando pontos chaves sobre privacidade e segurança, o autor defende a ideia de que na reforma do GDPR é prescrito o que a empresa precisa fazer para se adequar, mas não indica como realizar essa implementação, deixando uma margem muito grande para diferentes interpretações. Desse modo, sua hipótese inicial era de que as organizações estariam o mínimo possível em conformidade com o GDPR, apenas para evitar multas.

Para Imrichová, a finalidade das políticas de privacidade é estabelecer um programa global que gerencie e organize a coleta, compartilhamento e processamento dos dados, criando uma governança que esteja apta a garantir a conformidade da empresa com as leis, garantindo que a coleta, compartilhamento e processamento desses dados seja feita de forma legal. As políticas de privacidade de dados são diferentes em cada organização e se baseiam em limites geográficos ou de negócios, mudando de acordo com a área de atuação da organização. Isso pode resultar em uma política de privacidade de dados muito complicada para grandes corporações multinacionais com diversas operações comerciais.

Embora o GDPR tenha uma lista de requisitos que as empresas devem seguir, não é prescritivo. A lei não se concentra nas formas ou soluções que as empresas podem escolher para implementar os padrões de operações. Existem muitos métodos diferentes que uma empresa pode usar para garantir a segurança dos sistemas, e é comum que estes variem de acordo com o porte da organização e o orçamento destinado para esse fim. Por outro lado, é possível observar uma vantagem, pois por não ser muito específico gera uma espécie de continuidade futura para o regulamento. À medida que novas técnicas

de proteção e tecnologias de segurança cibernética são desenvolvidas no setor, elas não precisarão ser referenciadas diretamente no GDPR, porém isso não significa que estar em conformidade com a lei será uma tarefa fácil.

Em sua pesquisa, realizada em Agosto de 2019, Imrichová coletou a perspectiva de 30 funcionários de cibersegurança das áreas de educação (1), finanças (5), saúde (11), segurança (3), manufatura (3), varejo (1) e tecnologia (6) sobre quais ferramentas estão sendo utilizadas e como as respectivas organizações estão adaptando seus planos de respostas a incidentes para entrar em conformidade com o GDPR. Pode ser observado os resultados obtidos na Figura 3. Nela é possível visualizar que 2 organizações não estão em conformidade e nem pretendem, 5 não estão em conformidade mas pretendem e 23 já estão em conformidade com a nova lei de proteção de dados. Desse modo, ao constatar que as organizações destinaram parte do orçamento de segurança da informação para ficar em conformidade com a nova lei, o autor defende uma nova hipótese: os processadores de dados veem valor na melhora do SOC, não apenas para entrar em conformidade com o GDPR mas também para gerar impacto na cibersegurança da organização.

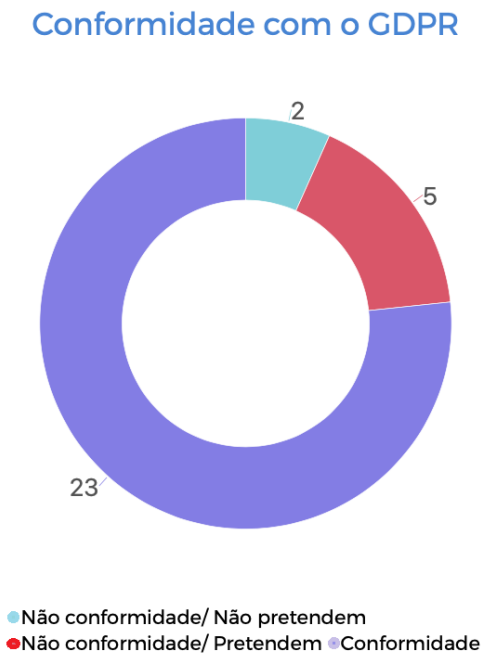

Figura 3: Gráfico de Conformidade com o GDPR.

Por fim, Imrichová defende a ideia de que quanto mais as organizações receberem multas provenientes do GDPR, mais investimentos serão feitos na área, gerando melhorias na coleta, armazenamento e proteção dos dados.

No artigo *"Early GDPR penalties - Analysis of implementation and fines through May 2020"* de Josephine Wolff e Nicole Atallah [12], o objetivo principal é a análise de ordens de execução emitidas por DPAs (autoridade de proteção de dados) durante os primeiros 24 meses do GDPR. Cada país que compõe a União Europeia tem autonomia dentro de seu território para determinar qual artigo da lei está sendo violado e qual o valor da multa a ser aplicada, pontos que foram objeto de análise do estudo.

No levantamento realizado por Wolff e Atallah e conforme podemos observar nas Figura 4 e Figura 5, os países com maior quantidade de multa foram Espanha (73), Romênia (27), Hungria (23), Alemanha (21) e Bulgária (19). Entretanto o levantamento de valor médio das multas é diferente, tendo o seguinte ranking: Reino Unido (£105.103.400), França (£10.220.000), Itália (£3.586.545) e Áustria (£2.581.443). A violação por base legal insuficiente para processamento de dados teve maior número de multas (98), seguida da violação por técnicas e medidas organizacionais insuficientes para garantir a segurança da informação (59). Apesar da quantidade de multas ser maior na primeira violação (£110.858.422), o valor total das multas é maior na segunda (£332.864.417). Os autores defendem a ideia que inicialmente o GDPR tinha como objetivo principal reforçar a privacidade dos usuários, mas com o tempo esse objetivo passou a focar na segurança da informação das organizações.

Outro ponto que deve ser ressaltado das penalidades impostas é que grandes empresas como Google, Amazon e Meta foram multadas desde que a lei entrou em vigor. Em Janeiro de 2019 a Comissão de Proteção de Dados da França multou o Google em £50.000.000 por falta de transparência na forma como os dados dos usuários são processados para a obtenção de anúncios personalizados [13]. Em Julho de 2021, a Comissão Nacional de Proteção de Dados de Luxemburgo multou a Amazon em £746.000.000 por não estar em conformidade com os princípios gerais de processamento de dados [14]. Em Março de 2022, a Comissão de Proteção de Dados da Irlanda impôs multa de £17.000.000 à empresa Meta, dona do Facebook, Whatsapp e Instagram, por não utilizar técnicas adequadas de medidas de segurança.

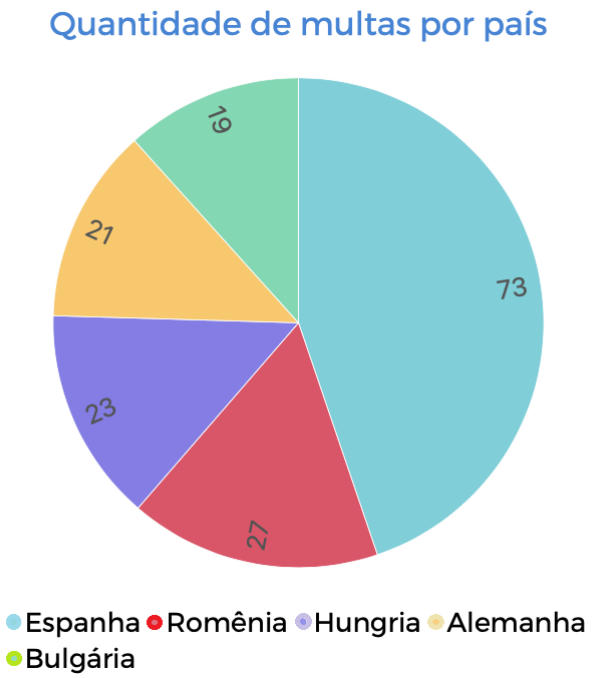

Figura 4: Quantidade de multas por país.

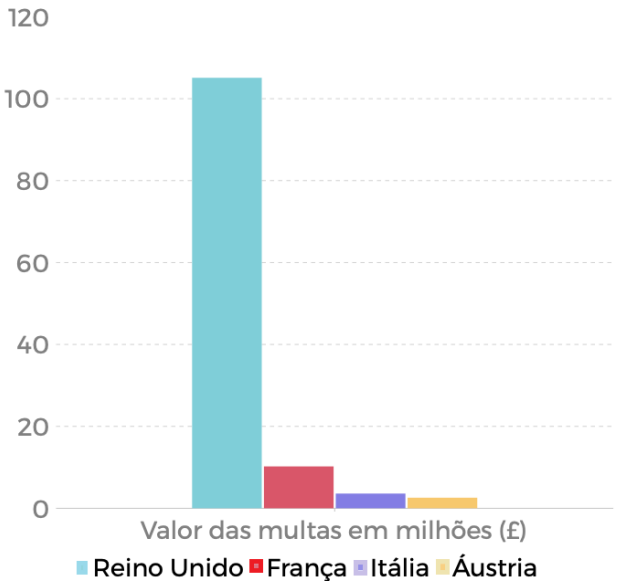

Figura 5: Valor das multas por país.

Todos esses estudos colaboram para a visão da efetividade do GDPR nas empresas, que, apesar de recente, já opera para o melhor tratamento e proteção de dados pessoais. Com a melhoria realizada pelas empresas nesse aspecto, percebe-se uma maior confiabilidade na segurança de cada organização.

2.2 Panorama da regulação de proteção de dados no Brasil

A Lei Geral de Proteção de Dados (LGPD) surge no Brasil como contraponto em relação às leis já estabelecidas, tendo influência direta do GDPR. No regulamento europeu é previsto que as transações internacionais de dados ocorram apenas com países que garantam um grau adequado de proteção de dados. Nesse contexto, a LGPD traz à tona a discussão acerca da proteção de dados e como isso influencia no comércio exterior. Diante da necessidade de uma regulamentação que padronize coleta, armazenamento e processamento dos dados e puna quem a descumpra, a nova lei brasileira é uma forma de alcançar essa garantia. Além da relação com o exterior, a LGPD também surge como uma proposta de adequação para o tratamento dos dados nas organizações nacionais tendo em vista que casos de ciberataques foram registrados recentemente, tanto em instituições públicas quanto em empresas privadas.

Sendo a primeira lei federal a regular o uso de dados pessoais e criar novos conceitos jurídicos específicos sobre o tema, a LGDP, como visto anteriormente, é uma resposta direta à entrada do GDPR em vigor, existindo muitos pontos de convergência entre ambas. Assim como o GDPR, a LGPD teve como fundamentos os princípios do respeito à privacidade, liberdade de expressão, de informação, de comunicação e de opinião; não violação da intimidade, honra e imagem; livre iniciativa, livre concorrência e defesa do consumidor e, principalmente, os direitos humanos [4]. Também é importante citar que no Brasil a não aplicabilidade da lei ao tratamento de dados pessoais realizado por pessoa natural com fins exclusivamente particular e não econômicos ou 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 na LGPD [4]. A Tabela 2 destaca os principais pontos da lei referentes à segurança da informação.

Tabela 2: Princípios da LGPD referentes à segurança da informação.

Artigo	Descrição
Art 6°. VII	As atividades de tratamento de dados pessoais deverão observar a boa-fé na utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
Art 6°. VIII	As atividades de tratamento de dados pessoais deverão observar a boa-fé na adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
Art 6°. X	As atividades de tratamento de dados pessoais deverão observar a boa-fé na demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.
Art 9°. III	O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados bem como a identificação do controlador
Art 46°	Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
Art 48°	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.
Art 50°	Os controladores e operadores, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento.

No artigo *"Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD"*, de Abigayle Erickson [16], a autora aponta as similaridades e diferenças entre o regulamento brasileiro e europeu. Quando comparada com o GDPR, a LGPD é menor e menos restritiva, possibilitando flexibilidade de interpretação para as autoridades. Dentre as diferenças é válido citar que a lei brasileira não é rígida quanto às notificações às autoridades já que um incidente de segurança que pode gerar riscos deve ser remetido à ANPD (Autoridade Nacional de Proteção de Dados) em um período razoável de tempo, novamente deixando margem para interpretações. Outra diferença que deve ser mencionada está na estrutura das multas, na lei nacional as organizações podem ser multadas em até 2% de seu faturamento no último exercício, sendo o valor limite de R$ 50.000.000, valor menos lesivo que o imposto pela lei europeia, que prevê multa de até £20.000.000 ou até 4% do faturamento anual da organização. A autora defende a ideia de que a falta de restrições, flexibilidade de interpretações e ausência de guias explicativos podem prejudicar as organizações a estarem em conformidade com a lei brasileira.

O artigo "Um panorama da implementação da LGPD no Brasil: uma pesquisa exploratória com 216 profissionais" de Lamara Ferreira e Marcelo T Okano [17], consiste de uma pesquisa realizada em 2021 com objetivo de verificar o panorama de adequação das organizações brasileiras para estar em conformidade com a lei. A pesquisa foi realizada com 261 profissionais de diversos segmentos do mercado, coletando a opinião de profissionais sobre a LGPD e as ferramentas e métodos para auxiliar na sua implementação.

Em um dos questionamentos da pesquisa, foi perguntado aos entrevistados se a organização já iniciou um projeto de adequação à LGPD. Na amostra estudada, 33,8% das empresas ainda não haviam iniciado um projeto de adequação à nova lei, enquanto 66,2% já haviam, conforme pode-se observar na Figura 6. Também foi feito um levantamento sobre as principais áreas envolvidas na implementação da LGPD dentro das organizações. Os entrevistados podiam selecionar mais de uma área. Tecnologia e Informação (118), Jurídico (112), Recursos Humanos (99), Administrativo (87) e Atendimento ao Cliente (85) foram as áreas com mais aparições. Além disso, a pesquisa também levantou os maiores desafios das organizações na adequação à LGPD. Cultura interna (100), Investimento em segurança da informação (85), Mapeamento de processos (67) e Investimentos da empresa (67) são os desafios com mais aparições. A partir dos resultados dessa pesquisa, é

possível ter uma ideia do atual panorama brasileiro.

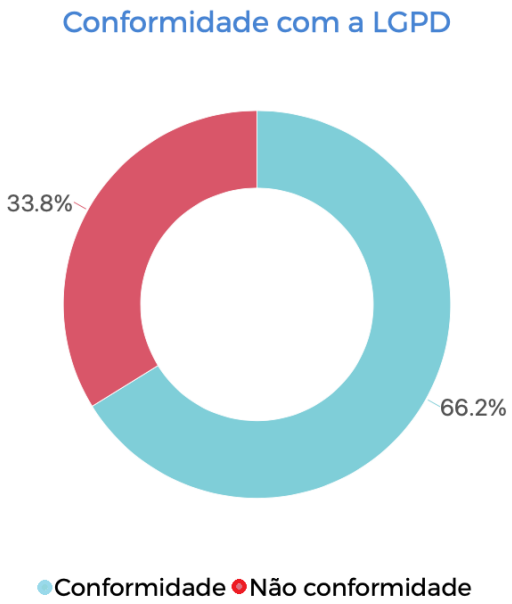

Figura 6: Gráfico de conformidade com a LGPD.

Outra pesquisa que corrobora com o estágio de implementação da LGPD no Brasil foi a realizada pelo Sebrae/SC [18] na qual várias empresas de pequeno porte foram entrevistadas com o objetivo de verificar o conhecimento e o nível de implementação da LGPD. A amostragem foi dividida em camadas. Nos resultados obtidos foi inferido que 74,5% das empresas sabiam quando a lei entraria em vigor. No que tange ao nível de conhecimento e adequação 22,6% já estão se adequando, 25,6% estão em fase de adequação, 19,5% não estão adequadas, 32,3% não conhecem sobre a lei. Em relação aos portes, as pequenas empresas são as que possuem maior entendimento da lei, com 80,8% de empresas que já ouviram falar, enquanto as micro empresas somam 74,2% e os MEI 's 47,5% nesta categoria. Por fim, conclui-se que a maioria das empresas já apresentam conhecimento da lei, mas que entrar em conformidade com a lei ainda é um desafio.

A primeira penalidade no Brasil ocorreu no dia 18 de Setembro de 2020, quando a empresa Cyrela foi multada em R$10.000 por infringir a LGPD [19]. No entanto, no dia 24 de Agosto de 2021, o Tribunal de Justiça de São Paulo (TJSP) reverteu, em segunda instância, a condenação da construtora Cyrela concluindo que não havia evidências suficientes que pudessem comprovar que o compartilhamento das informações foi realizado pela incorporadora [20].

Todos esses estudos colaboram para a visão de que a lei ainda é recente e sua flexibilidade para interpretações ainda dificulta um consenso no âmbito jurídico e a efetiva implementação nas organizações no âmbito segurança da informação. Portanto questionamentos surgem quanto a severidade das multas aplicadas, quanto a padronização no processamento dos dados e a disposição de investimento por parte das empresas para resolver os problemas identificados dentro das organizações.

2.3 Panorama geral de SOC

Dados os panoramas do GDPR e da LGPD com foco na segurança, também faz-se necessário abordar os conceitos que permeiam a segurança da informação, o qual está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização e possui como princípios básicos garantir disponibilidade, integridade, confidencialidade e autenticidade da informação [21].

- Disponibilidade: Este princípio garante que a informação esteja sempre disponível e acessível quando requerida por pessoas autorizados.
- Integridade: Este princípio garante que a informação recebida é a mesma informação que foi enviada, de modo que só pessoas autorizadas podem fazer alterações.
- Confidencialidade: Este princípio garante o sigilo da informação, garantindo que apenas pessoas autorizadas possam acessá-la.
- Autenticidade: Este princípio garante que a fonte da informação é verdadeira, ou seja, quem enviou a mensagem é quem alega ser.

Outro ponto importante que deve ser conhecido por parte das empresas são os ataques de redes. Um ataque de rede nada mais é que uma tentativa de invasão a uma rede com a finalidade de torná-la inacessível ou obter dados sigilosos. Dentre os principais ataques podemos citar o ataque de negação de serviço (DoS, do inglês *Denial of Service*), *phishing*, *ransomware*.

Um ataque de negação de serviço consiste em tornar um sistema indisponível por meio de sobrecarga de recursos em um computador ou servidor [21]. Já o *phishing* é um ataque de engenharia social que busca obter dados privados das vítimas [22]. Nesse

ataque, o atacante se passa por uma entidade de confiança da vítima, induzindo-a a lhe passar dados confidenciais. Por fim, o *ransomware* é um software capaz de bloquear um computador de modo que o atacante possa solicitar um resgate para desbloqueá-lo. Geralmente, por meio de engenharia social, o atacante induz a vítima a baixar um software malicioso em sua máquina, capaz de torná-la inacessível [23].

Para se defender de possíveis ataques, uma organização pode fazer uso de ferramentas e técnicas de segurança da informação como antivírus, *firewall* e becape [21]. Um antivírus é um software capaz de prevenir, detectar e eliminar vírus de um dispositivo. Um *firewall* é um dispositivo capaz de monitorar o tráfego entre a rede externa e interna de uma organização. Já o becape é uma cópia de segurança, que pode ser restaurada em caso de indisponibilidade da informação.

Nesse contexto de prevenção, detecção e eliminação de ameaças, temos o SOC, Figura 7, que além de atuar nessas ações, funciona também como uma instalação onde se encontram os profissionais de segurança da informação responsáveis por monitorar e analisar a postura de segurança de uma organização de forma contínua. Por meio de uma combinação de soluções de tecnologia e um forte conjunto de processos. Com mecanismos de correlacionamento, uma estrutura SOC é capaz de cruzar dados de eventos gerados nos recursos de segurança da organização como *firewalls*, IPs e antivírus, possibilitando que as tentativas de invasão sejam detectadas.

Figura 7: Aplicações de um SOC. Fonte: Autores, adaptado de [1].

Como visto na Figura 7, um SOC utiliza múltiplas técnicas para garantir a segurança da rede como agregação e correlação, coleção de logs, relatórios, pesquisa e desenvolvimento, inteligência de ameaças, conhecimentos básicos, alarmes e SIEM.

- Agregação e correlação: A combinação de dados para ampliar o entendimento do ambiente monitorado.
- Correlação de logs: É um registro contínuo, que contém a data e a hora do evento, além de uma mensagem criada automaticamente pelos sistemas para identificar padrões que possam ajudar na solução de problemas, nas previsões de desempenho, na manutenção e em melhorias.
- Relatórios: São responsáveis pela realização de um acompanhamento frequentemente com o objetivo de manter qualidade e eficiência.
- Pesquisa e desenvolvimento: É responsável pela busca de evolução nos sistemas de segurança, bem como o desenvolvimento dessas melhorias.
- Inteligência de ameaças: Processo de identificar e analisar ameaças cibernéticas.
- Conhecimentos básicos: É uma base onde fica armazenado documentação que inclui respostas a perguntas frequentes, guias de instruções e instruções de solução de problemas com o intuito de facilitar que os colaboradores encontrem soluções para seus problemas sem precisar pedir ajuda.
- Alarmes: São informativos de que há um comportamento inesperado no sistema.
- SIEM: É a combinação de gerenciamento de eventos de segurança (SEM – *security event management*) e gerenciamento de informações de segurança (SIM – *security information management*).

No livro *"Definitive Guide to SOC-as-a-Service"* [1], Crystal Bedell e Mark Bouchard definem o gerenciamento do ciclo de vida da segurança de uma empresa. Primeiramente temos a fase de identificação, onde é necessário a análise de riscos, as estratégias de gerenciamento desses riscos, a governança e o envolvimento de negócios. Na fase de proteção, tem-se o controle de acesso, segurança dos dados, tecnologias protetivas e a consciência junto da capacitação. Na fase de detecção, pode-se observar as anomalias e os eventos, a monitoração contínua e o processo de detecção desses incidentes. Logo após

a detecção, é mostrada a fase de resposta aos incidentes, que compreende a comunicação, o planejamento de resposta, a análise do ocorrido, a mitigação e a melhoria. Por fim o autor explana sobre a fase de recuperação, onde os pontos apresentados anteriormente são bem definidos para que sejam evitados novos ataques relacionados, encerrando assim o ciclo da segurança.

No artigo *"GDPR impact on Information Security Incident detection and response"* [11], Imrichová pontua como SOC e GDPR estão relacionados. Sabe-se que o GDPR pressiona as organizações a implementar medidas de segurança, já que em caso de violação, a empresa deve comprovar que os métodos de proteção em seu ambiente eram adequados. Para estar em conformidade com a lei as medidas de segurança devem seguir os seguintes requisitos: Proteção de dados, detecção de eventos de incidentes, respostas e relatórios. Desse modo, o autor defende a ideia de que investimentos em SOC podem resultar na redução de tempo para detectar e relatar uma violação de dados.

Também é observado no *"Definitive Guide to SOC-as-a-Service"*, a defesa da existência de 5 níveis de sistemas de segurança que as organizações podem implementar, conforme observado na Figura 8:

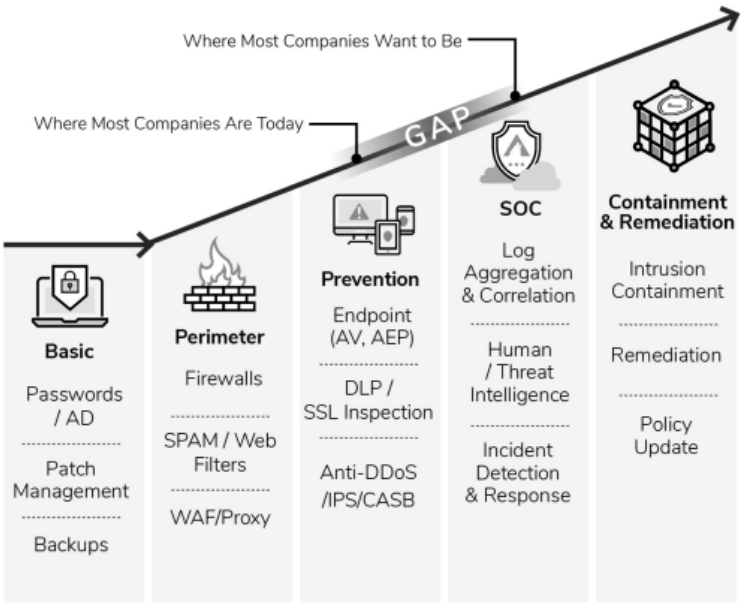

Figura 8: 5 Níveis de Sistemas de Segurança [1].

Analisando cada um dos pontos de forma separada, obtém-se:

1) Básico: Consiste do uso de senhas, gerenciamento de pacotes e becape;

2) Perímetro: Uso de *firewalls*, *proxies* e filtros de pacotes;

3) Prevenção: Ferramentas nas máquinas dos usuários como antivírus, inspeção SSL, anti-DDoS (*distributed denial of service*), IPS (Sistema de prevenção de intrusão) CASB (Corretor de segurança de acesso à nuvem);

4)SOC: Agregação e correlação de logs, sistema inteligente de detecção de ameaça, detecção e resposta a incidentes;

5)Contenção e remediação: Contenção de intrusões, reparação e política de atualizações.

2.3.1 Dificuldades de implementação do SOC e evolução

Apesar de um SOC permitir que uma postura de segurança madura seja alcançada, construir e gerir um SOC demanda custos e desafios que nem todas as organizações estão dispostas a enfrentar. No artigo *"Security Operations Center: A Systematic Study and Open Challenges"* [24], Manfred Vielberth, Fabian Böhm, Ines Fichtinger e Günther Pernul expõem os principais desafios para a implementação de um SOC em cada um dos seguintes segmentos: Pessoas, Processos, Tecnologias e Governança.

O segmento de pessoas define quais papéis e responsabilidades cada agente irá assumir. Trabalhar com respostas a incidentes demanda atenção e seriedade, pois um descuido pode gerar danos irreversíveis para a organização. Os principais desafios desse segmento envolvem atividades monótonas e desmotivadoras, falta de agentes capacitados e dificuldade de mantê-los na organização, já que, por existirem poucos no mercado, são cobiçados por outras empresas.

O segmento de processos é responsável por determinar as ações e como elas devem ser executadas. Em SOC os processos não são bem definidos, demandando que processos de outros setores preencham essa lacuna. Essa falta de processos definidos e necessidade de adaptar processos gerais para SOC são os principais desafios do segmento de processos.

O segmento de tecnologias é responsável por criar métodos de execução das atividades. O aumento da complexidade devido à implementação da infraestrutura, diversas fontes de dados e não estruturação dos mesmos causa necessidade de tratar esses dados antes de chegar em uma solução propriamente dita e é um dos grandes desafios desse segmento. Além disso, a grande variedade de ferramentas é outro desafio, pois estas pre-

cisam estar configuradas corretamente e com a manutenção em dia para que não causem incidentes do tipo falso positivo. Por fim, a dificuldade de automatizar as tarefas de um analista causa um baixo nível de automação nos SOC, gerando muitas demandas manuais e repetitivas e diminuindo a eficiência do tratamento de incidentes.

Medir a performance de um SOC é uma das tarefas mais importantes do segmento de governança, entretanto permanece como um dos desafios já que as métricas utilizadas atualmente são consideradas ineficientes. Além disso, a falta de boas práticas e padrões bem como as novas regulamentações de privacidade completam as maiores adversidades desse segmento.

Embora o cenário apresentado até o momento exponha desafios e dificuldades com relação à implementação de um SOC, estudos recentes apresentam evoluções para essas dificuldades. No artigo *"Next Generation Security Operations Center"* [25], Otto Lindström traz à tona a discussão que o avanço da cibersegurança tem forçado o SOC a evoluir, para que ele possa defender as organizações das ameaças presentes e futuras. Defender de forma reativa não é mais suficiente, agora a missão principal do SOC deve ser estabilizar e manter a situação de cibersegurança da empresa.

Visando a melhoria nos blocos de construção das unidades SOC (pessoas, processos e tecnologia), visto que muitos dos procedimentos realizados antigamente não são mais eficientes em combater as novas ameaças e o número de alertas tornou-se exaustivo a ponto de que investigar todos eles está além da capacidade de analistas humanos. Otto sugere quatro tipos de mudanças que fornecerá uma consciência situacional.

O primeiro ponto de mudança sugerido pelo autor é alteração da visão do processo de Reativo para Proativo. Historicamente, o SOC tem sido principalmente reativo atuando somente depois da descoberta da ameaça. Porém, quanto maior o número de ameaças e quanto mais perigosas mais difícil isso se torna de ser controlado. A partir dessa análise faz-se necessário que o SOC se torne cada vez mais proativo, os ataques estão acontecendo de forma muito rápida e geralmente não há tempo hábil para reagir ao ataque. Para mudança de panorama deve-se desenvolver processos para uma análise contínua de ameaças, criando assim uma consciência situacional. Como exemplo, o autor mostra que para melhorar essa proatividade pode realizar uma verificação ativa na rede e a criação de um sistema que busque por vulnerabilidades conhecidas, para que haja atualizações ou implementação de algumas precauções antes que essas vulnerabilidades

sejam exploradas por um invasor.

Logo em seguida, outro ponto sugerido pelo autor é a automatização das defesas. Junto com o avanço em segurança da informação tem-se o avanço nas técnicas de ataque, que constantemente estão melhorando suas táticas de forma a enfraquecer o sistema de medidas de defesa estáticas. Por mais que esses métodos de defesa não sejam mais tão eficazes, eles ainda são úteis, pois ainda conseguem detectar ataques básicos. A popularidade da Inteligência Artificial (IA) surge como uma solução para essa questão, pois ao mesmo tempo que a auto aprendizagem do algoritmo se adapta a diferentes situações ele também aumenta sua precisão ao longo do tempo, tornando as defesas mais fortes e mais ágeis no combate às ameaças. Apesar de todo esse benefício adquirido por utilizar aprendizado de máquina, é importante salientar que apenas essa técnica de detecção pode causar muitos falsos negativos ou falsos positivos, então é aconselhado sempre usar essa técnica associada a uma ferramenta de detecção estática, para que torne a segurança, além de rápida, eficaz.

O terceiro ponto deste estudo é a automação inteligente de ameaças. Estar ciente das ameaças mais recentes ajuda as unidades SOC a se inclinarem para uma defesa proativa. Mas é importante citar que deve-se coletar informações importantes, pois diariamente são descobertos em uma organização diversos tipos de ameaças, portanto é necessário filtrar as que são relevantes, para que não haja uma saturação na lista de informações.

Por fim, o autor cita como ponto de melhoria para a nova geração do SOC a Internet das Coisas (IoT) e a Computação em Nuvem. Os dispositivos IoT estão se tornando cada vez mais populares, pois mais aplicativos estão sendo desenvolvidos para esses sistemas de computação que utilizam o baixo consumo de recursos. É inevitável que esses dispositivos se tornem parte de uma rede normal. Em um futuro próximo, a grande quantidade de dispositivos IoT irá gerar uma quantidade muito grande de dados. Isso deve ser considerado na implementação das unidades SOC, pois elas deverão ser capazes de processar os dados gerados pelos dispositivos IoT. Caso contrário, o SOC não poderá manter uma imagem situacional da segurança. Outro desafio apresentado nessa análise que deve ser considerado é o crescente uso de computação em nuvem. A computação em nuvem indica que uma alta demanda por recursos deve estar disponível, para isso muitas empresas alugam provedores desse serviço. O foco do estudo de Otto está na nuvem

pública em vez da privada devido aos desafios que ela cria. Ao usar a nuvem pública, as organizações têm autoridade limitada sobre as redes do provedor de nuvem. Isso significa que a organização pode não conseguir ver o que acontece na nuvem, no entanto muitos sistemas modernos conseguem implantar um coletor de logs na nuvem, para que haja uma verificação do aconteceu com os dados enquanto eles trafegavam na Internet. Essa solução só se faz necessária em casos de uso extensivo da nuvem ou quando a organização não possui capacidade de armazenar seus serviços localmente.

Mesmo apresentando pontos a melhorar, o SOC ainda é uma ferramenta viável para a segurança da empresa. Devido ao fato de atuar com proteção de dados, detecção de eventos de incidentes, respostas e relatórios, a unidade SOC contempla os requisitos exigidos para que estejam adequados aos regulamentos. Portanto, todos esses estudos e mecanismos possibilitam que essa estrutura colabore para a efetividade da implementação dos regulamentos nas organizações.

3 DISCUSSÃO E ANÁLISE

3.1 Comparação entre GDPR e LGPD

Dado a comparação do GDPR e LGPD feita por Abigayle Erickson em "*Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD*" [16], é possível elencar os pontos de divergência dos dois regulamentos, colocando em pauta aquilo que julga-se necessário para melhoria em cada um dos casos. Para tal análise foram listados os pontos divergentes mais importantes de cada um dos regulamentos na Tabela 3.

Tabela 3: LGPD vs GDPR

Situação	GDPR	LGPD
Quanto aos casos permitidos no regulamento	Prevê permissão para processamento dos dados nos casos de consentimento do proprietário, execução contratual, compliance ou conformidade, interesse vital, interesse público e interesse legítimo.	Mais ampla, incluindo também estudos de órgãos e agências de pesquisa, exercício regular de direitos em processos judiciais, proteção ao crédito e proteção à saúde.
Quanto ao vínculo entre controlador e operador	Exige um contrato ou vínculo jurídico entre controlador e operador.	O operador deve realizar o tratamento dos dados de acordo com as instruções do controlador.
Quanto às multas	Limita as multas em £20 milhões ou até 4% da receita da empresa no ano anterior, optando-se pela que gere maior dano financeiro à empresa.	Estipula que a multa deve ser de até 2% da receita da empresa no ano anterior, sendo o limite de R$ 50 milhões.

Quanto aos incidentes e vazamentos	Prevê que as empresas devem notificar a autoridade competente dentro do prazo de 72 horas.	Não estipula um prazo, mas determina que, além da autoridade, os titulares dos dados também devem ser notificados.
Quanto à fiscalização	Define que cada país deve possuir um *Data Protection Authority* (DPA), responsável por verificar se as organizações estão em conformidade.	Não foi definido um DPA, mas criado a Autoridade Nacional de Proteção de Dados (ANPD) que funciona de uma forma semelhante da DPA.

Após a realização da comparação, percebe-se que alguns pontos necessitam de uma revisão, para que atuem de melhor forma e mais segura. A lei brasileira é mais permissiva com relação aos casos de tratamento de dados. Permitir tratamento de dados no que se refere à saúde pode ser benéfico para a sociedade, possibilitando que levantamentos sejam feitos em casos de necessidades extremas, como a pandemia do covid-19. Outro caso a ser citado também é a questão de proteção do crédito, pois se houver inadimplência por parte do titular dos dados, poderá ser realizada uma operação de consulta aos dados pessoais, em sistemas como o Serviço de Proteção ao Crédito (SPC).

Apesar de ser mais ampla com as hipóteses de tratamento de dados, a LGPD não é tão rígida na fiscalização quanto o GDPR. Ao prever vínculo jurídico entre controlador e operador, a lei europeia estabelece maior segurança aos stakeholders, pois todas ações serão definidas em contrato, garantindo a responsabilização de quem pratica atos fora do escopo do contrato. Isso reflete diretamente na notificação em casos de incidentes e vazamentos de dados, outro ponto de divergência entre os regulamentos. O GDPR exige que as empresas notifiquem a autoridade competente dentro do prazo de 72 horas. Por não haver a necessidade de contrato, não é estipulado um prazo para notificação por parte das empresas brasileiras, apenas que deve ser informado às autoridades e ao titular dos dados.

A partir da comparação entre os regulamentos, se faz necessário também a comparação entre suas aplicações e fiscalização. No caso do GDPR pode-se observar que as

multas são aplicadas de forma mais rigorosa, optando sempre pela que será mais danosa à empresa, já na lei brasileira é estipulado um limite de 2% da receita do ano anterior, não ultrapassando o valor de R$50 milhões.

O levantamento feito por Wolf e Atallah no artigo "*Early GDPR penalties - Analysis of implementation and fines through May 2020*" [12], junto das fontes informativas [13, 14, 15, 19, 20], permitem inferir que enquanto o GDPR já está penalizando quem o infringe, no Brasil ainda não é rígido com quem discumpre a LGPD. Um fator que reforça a ideia de maior rigidez na europa é utilização da ferramenta GDPR Enforcement Tracker [9] que informa as multas já aplicadas, filtrando por país, valor, artigo violado e empresa, conforme pode-se observar na Figura 9. Embora o primeiro caso de justiça da lei brasileira tenha ocorrido no ano de 2020, ano de sua entrada em vigor, não houve condenação da empresa acusada [20]. Além de reforçar a ideia de rigidez do regulamento de proteção de dados europeu, o levantamento também corrobora para a tese de que uma boa implementação segurança da informação é fundamental para estar em conformidade com a lei.

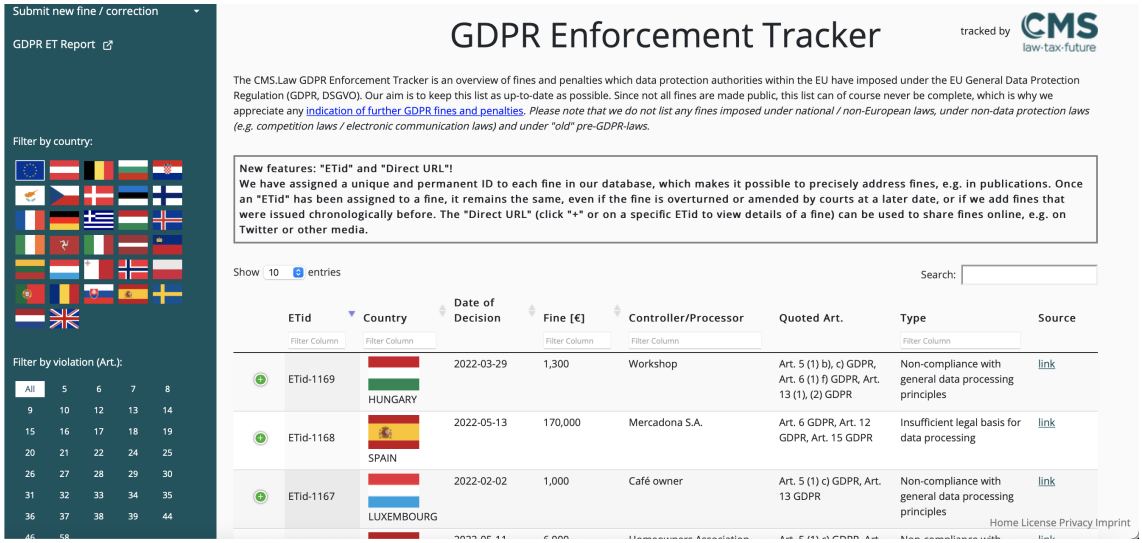

Figura 9: GDPR Enforcement Tracker [9].

Como já citado, a LGDP veio em resposta ao GDPR, pois no regulamento europeu é sucinto em dizer que outros países que possuem relações comerciais com empresas europeias, devem possuir uma política de proteção de dados que esteja em conformidade com o GDPR. Diante disso, alguns questionamentos são levantados: A lei brasileira existe apenas por interesse comercial? As penalidades estão sendo efetivas? Por que a lei europeia

está sendo efetiva e a brasileira não?

O artigo "Um panorama da implementação da LGPD no Brasil: uma pesquisa exploratória com 216 profissionais" de Lamara Ferreira e Marcelo T Okano [17] e a pesquisa feita pelo Sebrae/SC [18] auxiliam na análise do atual cenário brasileiro, sendo norteadores para responder essas perguntas. Na pesquisa de Ferreira e Okano, foi levantado que 33,8% ainda não haviam iniciado um projeto de adequação à nova lei, e as maiores dificuldades apontadas pelos entrevistados foram cultura interna, investimento em segurança da informação, mapeamento de processos e investimentos da empresa. Já a pesquisa do Sebrae esteve diretamente relacionada ao conhecimento da lei por parte das empresas, os resultados obtidos pela pesquisa sugerem que aproximadamente 51,8% das organizações não estão adequadas ou não conhecem a lei.

Portanto, a partir dos resultados obtidos dessas pesquisas, podemos inferir que os maiores desafios que acompanham a LGPD são a recente sanção da lei, a cultura interna das organizações, a penalidade branda e os investimentos na área.

Entendemos que por ser uma lei que foi criada recentemente a LGPD ainda é pouco difundida em território nacional, composto majoritariamente por empresas de pequeno e médio porte que não possuem conhecimento ou capacidade para regularização da norma em vigor. Por isso grande parte das empresas ainda estão em estágio inicial de implementação, enquanto outras desconhecem do que se trata. Como consequência, a cultura interna se apresenta como uma dificuldade, pois a mudança no processamento dos dados, bem como a necessidade de mapeamento de seu ciclo de vida, interfere diretamente no que já era um hábito consolidado no tratamento dos dados, sendo agora uma obrigatoriedade das empresas. Um exemplo de situação comum era o compartilhamento de dados pessoais de forma imprudente dentro das organizações, como a troca de informações entre setores.

Além dos desafios citados, a baixa fiscalização e branda penalidade influenciam diretamente na falta de investimentos em adequação à LGPD por parte das organizações. Em comparação com o GDPR, percebemos que a LGPD deixa lacunas para que a ANPD possa preencher no que se refere à fiscalização, causando atraso na efetividade do cumprimento da lei. Além dos altos valores das multas no GDPR, a rápida adesão do regulamento europeu também se deu pelo fato da aplicabilidade dessas multas às empresas que não estavam adequadas, o que é algo que não se observa por parte da ANPD. Consequentemente, as empresas brasileiras destinam menos recursos financeiros para os setores responsáveis

pela adequação do tratamento de dados, impactando na falta de profissionais capacitados na área.

Por fim, entendemos que a lei não veio somente para fins comerciais, mas por ser recente ainda demanda um tempo para maior difusão em território nacional. Diante do contexto apresentado nota-se que os desafios que acompanham a LGPD geram um déficit de utilização de ferramentas que facilitariam a implementação dos processos exigidos pela lei. O que nos leva ao próximo ponto a ser discutido: Diante das dificuldades de cumprimento dos regulamentos, o SOC é uma solução?

3.2 SOC e a LGPD

Ao tratar o assunto da regulação de proteção de dados é importante relacioná-lo com a segurança da informação. Apesar de ser uma lei voltada para o direito de privacidade, o uso de ferramentas de segurança auxiliam no processo de adequação das organizações aos artigos 6°, 9°, 46°, 48° e 50° da lei. Nesse contexto, a unidade SOC surge como candidata de solução para o cumprimento desse novo desafio que foi gerado a partir de discussões acerca de privacidade e segurança.

Na definição de Crystal Bedell [1], os logs de um SOC, por meio de sistemas inteligentes, atuam na detecção de ameaças e respostas a incidentes. No artigo "*GDPR impact on Information Security Incident detection and response*"[11], Imrichová defende a ideia de que investimentos em SOC podem resultar na redução de tempo para detectar e relatar uma violação de dados. Proteção de dados, monitoramento contínuo, detecção de eventos de incidentes, respostas e relatórios são requisitos para que uma organização esteja em conformidade com a lei.

3.2.1 Atuação do SOC em redes corporativas

Levando em conta a importância da segurança da informação para a Lei Geral de Proteção de Dados, nesta seção serão apresentados três cenários corporativos: uma empresa com baixo nível de segurança, uma empresa com médio nível de segurança e uma empresa com alto nível de segurança. Nessa análise será levado em consideração vulnerabilidades, possíveis ataques e ferramentas de proteção, bem como a atuação da lei na privacidade de dados pessoais.

No primeiro cenário, Figura 10, é apresentada uma arquitetura com nível de segurança baixo. A maior parte das empresas brasileiras são compostas de organizações de pequeno e médio porte. Sabendo disso, esse cenário tem como função representar a arquitetura de segurança dessas empresas, que se assemelham ao sistema de segurança de nível 2, perímetro, conforme a escala mencionada no panorama geral do SOC. Para fins de análise, supomos que essa rede corporativa seja de uma *startup* de consultoria, que armazena informações sensíveis dos clientes dentro do seu site. É necessário ressaltar que o site foi desenvolvido por terceiros e não há colaboradores na área de tecnologia. A segurança é simples, realizada apenas por um *Firewall* com filtros e regras de acesso. Nota-se também que a empresa possui uma quantidade limitada de colaboradores.

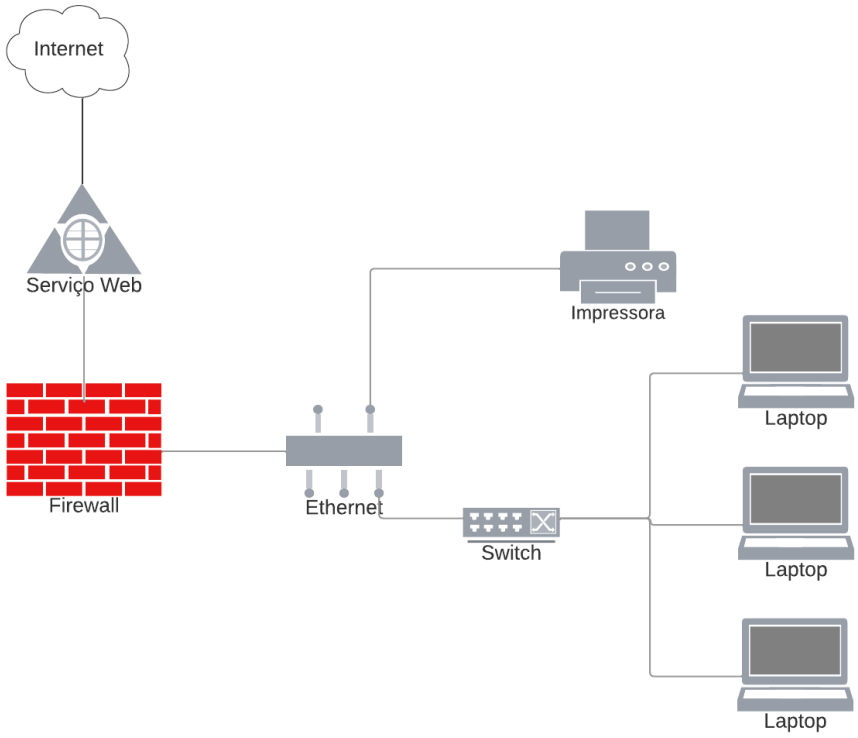

Figura 10: Rede corporativa com nível de segurança baixo.

Por se tratar de uma organização com uma quantidade de colaboradores limitada, torna-se mais fácil controlar e prevenir descuidos que fazem parte da segurança física, como esquecer o computador aberto em uma página de acesso restrito ou deixar a senha do colaborador visível. Além das vulnerabilidades físicas e humanas, há também outros tipos de vulnerabilidades ocasionadas por falta de uma equipe de tecnologia. O banco de dados armazenado no próprio serviço web deixa a empresa suscetível a vazamento dos dados em caso de invasão. A falta de antivírus expõe o computador dos colaboradores a acessos

indevidos. Outra brecha na segurança importante está relacionada com a comunicação da empresa, a utilização de *softwares* não homologados pode acarretar em fraudes e vazamento de informações sensíveis. Por se tratar de uma pequena empresa, não há uma política de controle de acesso, todos colaboradores têm acesso a todas informações. Há também uma falta de resposta a incidentes em caso de anormalidades na rede.

Todas essas vulnerabilidades expõem a empresa a ação de atacantes que tem como objetivo obter informações sensíveis para uso ilícito. Uma forma de ataque pode ser realizada através do e-mail corporativo, como um *phishing* ou um *ransomware*. Em um ataque do tipo *phishing*, o atacante pode simular um serviço confiável e a partir disso obter acesso a dados sensíveis. Nesse caso, pela falta de política de controle de acesso, o atacante teria circulação livre à rede interna da empresa. Já o *ransomware*, poderia ser facilmente enviado a um colaborador em uma das redes de comunicação não homologadas, ocasionando a obtenção dos dados por parte do atacante e a indisponibilidade de acesso por parte da empresa.

A partir da análise das vulnerabilidades e dos possíveis ataques, a Tabela 4 mostra quais pontos da LGPD estão sendo infringidos nesse cenário.

Tabela 4: Artigos infringidos no cenário de nível de segurança baixo

Situação detectada	Artigo infringido da LGPD
Infraestrutura de segurança	Infringe o Art. 6, X: Não há demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais
Falta de equipe de tecnologia	Infringe o Art. 9, III: Não há controlador nem operador de dados pessoais
Banco de dados armazenado no serviço web, falta de antivírus, utilização de *softwares* não homologados e falta de política de controle de acesso	Infringe o Art. 46: Não há adoção de medidas de segurança e técnicas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Falta de resposta a incidentes	Infringe o Art. 48: Gera uma demora na notificação de um incidente de segurança à Autoridade Nacional e ao titular
Falta de controle de acesso e governança	Infringe o Art. 50: Não há uma formulação de regras de boas práticas e de governança que estabeleçam as condições de organização, regime de funcionamento e procedimentos, além de normas de segurança, padrões técnicos e obrigações específicas para os diversos envolvidos no tratamento de dados pessoais

Para que haja evolução no cenário de nível de segurança baixo é necessário a implementação de medidas de defesa. Primeiramente, a criação de uma equipe de TI ou a contratação de serviço de terceiros, responsável pela organização de políticas de governança, pela melhoria na infraestrutura de segurança e pela definição de acessos. Além desses pontos, é necessário definir um controlador e um operador de dados pessoais. Para auxiliar nessas mudanças deve ser feito também investimento em ferramentas de comunicação e plataformas que operam sobre resposta a anomalias, pela geração de alarmes que informam a equipe especializada sobre incidentes.

Neste segundo cenário, Figura 11, é apresentada uma arquitetura com nível de segurança médio. Nessa arquitetura, é possível classificar o nível de sistema de segurança como sendo o nível 3, prevenção, onde apresenta maior robustez que o cenário mencionado anteriormente. Para fins de análise, supomos que seja uma empresa de saúde que atende o Brasil todo com filiais e acesso aos dados pessoais de vários colaboradores. É possível perceber que nessa organização há uma divisão por departamentos, além de um servidor de banco de dados separado e uma zona desmilitarizada (DMZ, do inglês *Demilitarized Zone*), que tem como função dar acesso aos serviços da empresa de forma externa, como por exemplo o servidor de emails. A segurança é realizada por um *Firewall* externo, onde é possível aplicar filtros e regras de acesso e as máquinas dos colaboradores possuem antivírus, Sistema de prevenção de intrusão (IPS, do inglês *Intrusion Prevention System*) e inspeção SSL.

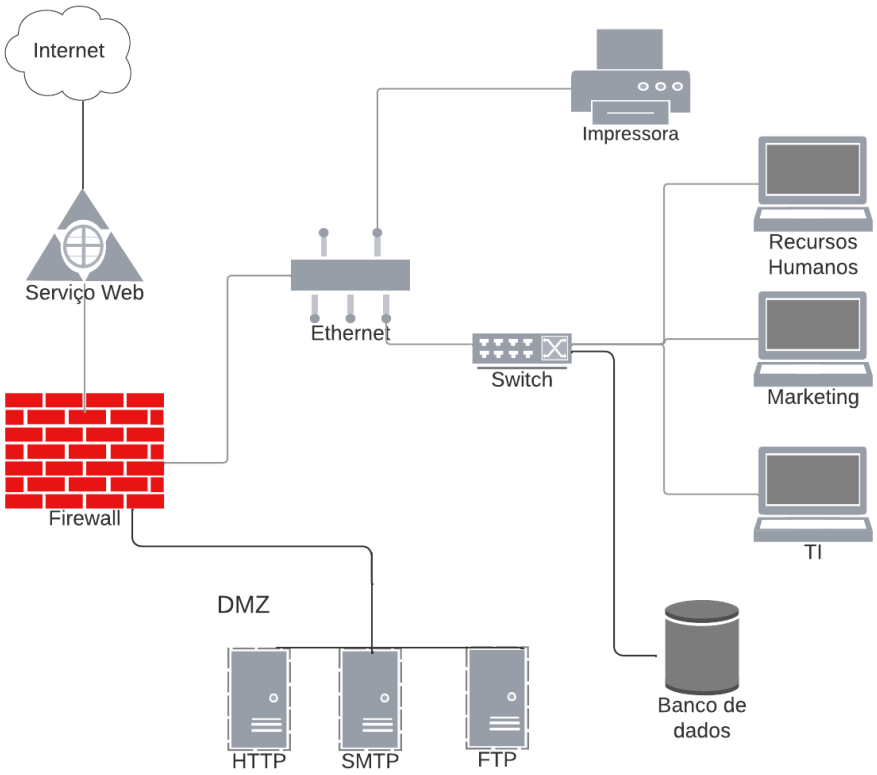

Figura 11: Rede corporativa com nível de segurança médio.

Por se tratar de uma organização que tem uma quantidade maior de colaboradores torna-se mais difícil controlar e prevenir descuidos que fazem parte da segurança física, podendo acarretar em vazamento de informações por parte de colaboradores que não estejam alinhados com a política de segurança da empresa. Apesar de ser uma organização com equipe de TI, com política de controle de acesso, infraestrutura de segurança bem definida e com operador de dados pessoais, ainda há vulnerabilidades na rede devido a falta de agregação e correlação de logs, sistema inteligente de detecção de ameaças e detecção e resposta a incidentes.

É importante destacar que nenhuma ferramenta é capaz de proteger totalmente uma organização de ataques provenientes de engenharia social. Nesse contexto, diante das vulnerabilidades expostas, caso um colaborador seja vítima de um ataque de *phishing* ou *ransomware*, a fonte deste incidente não será facilmente detectada pela equipe de TI possibilitando a permanência do atacante na rede, gerando maior dano à empresa. Entretanto, devido ao controle de acesso, os dados disponíveis ao atacante são limitados. Ainda nesse cenário, outro ataque que pode acontecer é o DoS, que gera a indisponibilidade

do serviço oferecido pela organização.

Mesmo que neste cenário apresente uma equipe de TI, protegendo de incidentes relacionados ao vazamento das informações, ainda há artigos da LGPD que necessitam ser implementados. Conforme apresentado na Tabela 4, a empresa do cenário de nível de segurança 3 infringe o Art. 48, pois a falta de resposta a incidentes gera uma demora na notificação à Autoridade Nacional e ao titular em caso de invasão.

Para que haja evolução nesse cenário é necessário realizar investimentos na equipe de TI, com maior especialização em segurança da informação e gerência de redes. Além disso, ferramentas de detecção de ameaças, serviços de log e alarmes são fundamentais para garantir um sistema de proteção de dados mais efetivo. Outra técnica para aumentar o nível de segurança seria a implementação da DMZ *dual firewall*, que adiciona uma camada extra de segurança entre rede interna e externa sendo denominado como defesa em profundidade.

Neste terceiro cenário, Figura 12, é apresentada uma arquitetura com nível de segurança alto. Para essa arquitetura, é possível classificar o nível do sistema de segurança como sendo de nível 4, SOC, que possui maior entendimento de segurança, além de um sistema dd detecção e resposta a incidentes. Para fins de análise, supomos que a empresa analisada seja uma empresa nacional que possui negócios também com o exterior, sendo assim armazena informações de vários clientes e também dos parceiros. Nessa organização percebe-se, além dos elementos informados no cenário anterior, um acréscimo de uma equipe de segurança e uma gerência para monitoração da rede. A segurança é complementada pela presença do SOC, que aumenta a capacidade de detecção de ameaças, gerando logs que serão utilizados para a criação de um padrão com a função de prevenir novos ataques.

Por se tratar de uma organização de maior porte e que possui negociações nacionais e internacionais, demanda uma grande quantidade de colaboradores. Devido a sua infraestrutura de segurança ser bem madura, por ter implementado o SOC, poucas são as vulnerabilidades encontradas. Entretanto, é sempre importante ressaltar que nenhuma ferramenta protege totalmente de ataques, já que ainda estão sujeitos a técnicas de engenharia social, como citado anteriormente nos outros cenários.

Outro aspecto da segurança alta é o becape, não apenas pelo fato do armazenamento separado para recuperação de dados perdidos, mas também no sentido de definição

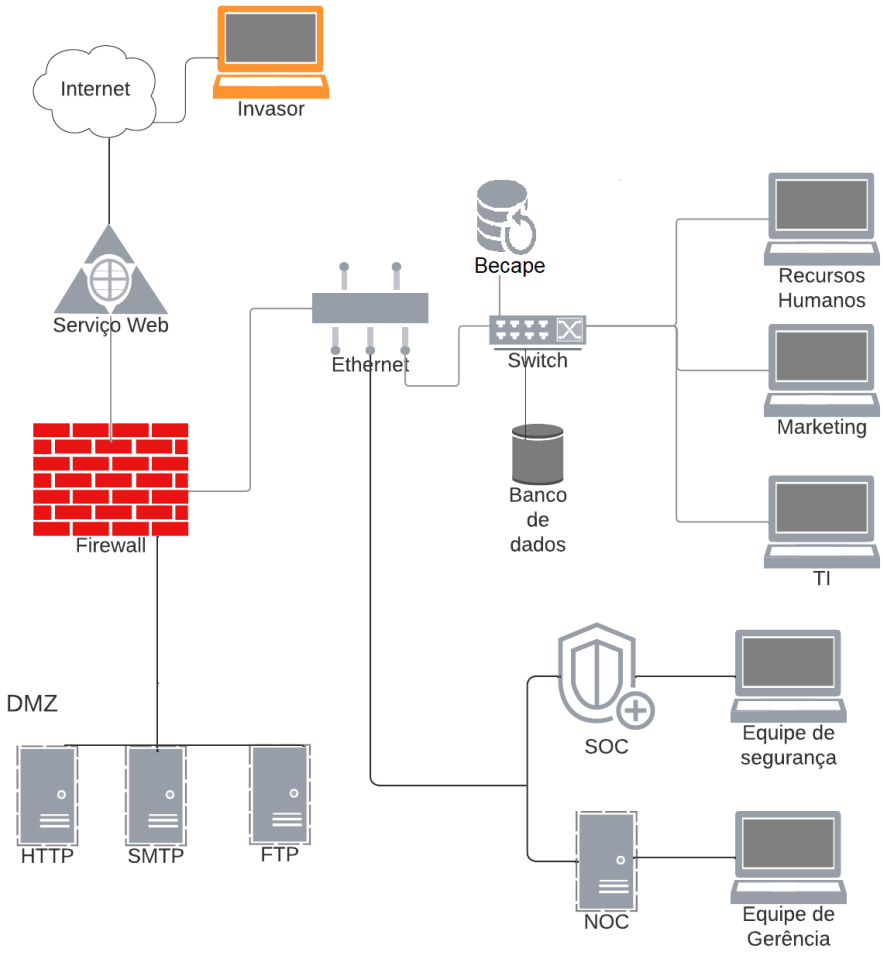

Figura 12: Rede corporativa com nível de segurança alto.

da segurança dos dados armazenados, estabelecendo protocolos de acesso para que somente a equipe de TI, com uso de criptografia, tenha permissão de fornecer dados do bacape quando solicitado. Nos outros cenários não há preocupação com a segurança das informações armazenadas, o que acarreta em problemas caso haja algum ataque ou transferência de informações do becape, pois o sistema estaria completamente vulnerável e suscetível ao roubo de dados pessoais.

É importante ressaltar que para a realização de negociações internacionais, a empresa deve estar de acordo com a LGPD, pois o GDPR impõe que os países que realizam negociações com a União Europeia devem possuir políticas de proteção de dados pessoais. No que tange a infringimento da lei, este cenário não possui descumprimento, apesar de que pode acontecer o vazamento de informações.

Diferentemente do que ocorre nos cenários simples e médio, este terceiro cenário implementa mecanismos de defesa que resolvem a maior parte dos problemas citados. Na

Tabela 5, é mostrado como é realizado o cumprimento da LGPD.

Tabela 5: Como o cenário de nível de segurança alto atua no cumprimento da LGPD

Situação detectada	Como o cenário de nível de segurança alto atua
Infraestrutura de segurança	Cumpre o Art. 6, X: É apresentado ,através do SOC, a implementação de medidas eficazes de cumprimento das normas de proteção de dados pessoais
Equipe de tecnologia	Cumpre o Art. 9, III: É bem definido o controlador e operador de dados pessoais, pois possui equipe especializada na Segurança e Gerência.
Banco de dados armazenado em local seguro, implementação de anti-vírus, utilização de *softwares* homologados e conjunto de políticas de controle de acesso	Cumpre o Art. 46 e Art. 50: A equipe de segurança é responsável pela definição de medidas e técnicas aptas a proteger os dados, atuando em conjunto com a equipe de governança que define os padrões de boas práticas junto ao tratamento desses dados. Além disso, o SOC tem como um princípio a base de conhecimento, com o objetivo de documentar procedimentos que auxiliam os funcionários na manutenção de suas ferramentas, deixando-as sempre atualizadas.
Resposta a incidentes	Cumpre o Art. 48: A partir da implementação do SOC é possível o cumprimento desse artigo através dos princípios de possuir plataformas que gerem alarmes em caso de anormalidades, a correlação dos logs para entender o momento do incidente e sua fonte, a agregação e correlação dos dados que gera uma prevenção de possíveis recorrências e os relatórios que fornecem o acompanhamento de todo tratamento para a manutenção da eficiência.

As possíveis ferramentas e mecanismos que podem ser utilizadas no cenário de alto nível de segurança estão elencadas a seguir:

- SIEM: Vinculado ao SOC, a plataforma tem como finalidade o gerenciamento dos eventos e informações de segurança. Podendo definir relatórios, base de conhecimento, pesquisa e desenvolvimento, correlação de logs, dentre outros;
- Kibana / Elasticsearch: Responsável pelo armazenamento de métricas e logs de dados em tempo real;
- Zabbix e Cacti: Ambas ferramentas são responsáveis pelo monitoramento de infraestrutura de TI, como redes, servidores, máquinas virtuais e serviços em nuvem.
- Pfsense: É uma solução de segurança *firewall* baseada em software, capaz de realizar a filtragem de conteúdo entre rede interna e externa;
- Snort: É um *software* de detecção de intrusão, capaz de perceber ataques por meio de padrões;
- Criptografia: A técnica de criptografia pode ser utilizada ao armazenar os dados no banco ou na comunicação entre serviços. Desse modo, em caso de invasão o atacante não terá acesso aos dados originais;
- Autenticação em duas etapas: Caso um atacante consiga acesso a senha de rede do colaborador, encontrará uma camada a mais de segurança para que consiga acessar os recursos da organização;
- NMAP: Realização de varredura contínua nas portas da rede buscando brechas e gerando alarmes para bloqueio de tráfego na porta.

3.2.2 SOC como solução na conformidade da LGPD no contexto de segurança da informação

Relacionando a definição de SOC, a análise dos cenários apresentados, a ideia defendida por Imrichová e os requisitos presentes na lei, entendemos que de fato todos esses pontos estão interligados e, investimentos na área de tecnologia, principalmente em SOC geram impacto na atuação de combate a incidentes envolvendo dados pessoais, sendo

objetos facilitadores de cumprimento da lei. Dessa forma, concluímos que o uso de SOC é uma possível solução para as dificuldades apresentadas na implementação da LGPD no âmbito de segurança da informação.

Apesar de ser uma possível solução, implementar uma unidade SOC ainda é um desafio. Devido a sua baixa popularização e sendo utilizado geralmente por grandes organizações, investimentos nessa área costumam ter alto custo. No artigo "*Security Operations Center: A Systematic Study and Open Challenges*" [24], Manfred Vielberth, Fabian Böhm, Ines Fichtinger e Günther Pernul discutem os principais desafios para a implementação de um SOC. Percebemos que as dificuldades de implementar uma unidade SOC vão além dos custos, já que a falta de pessoas capacitadas, adaptação de processos gerais e a complexidade da infraestrutura corroboram para o déficit de segurança de dados nas organizações. Diante disso, o SOC não se enquadra em uma solução de curto prazo, é necessário que haja planejamento adequado para a implementação dessa solução.

Além das dificuldades de implementação de uma unidade SOC, há também brechas no modelo de SOC atual, que o tornam vulnerável para contemplar todos os requisitos da LGPD. No estudo "*Next Generation Security Operations Center*" [25], Otto Lindström sugere uma evolução no SOC para torná-lo ainda mais efetivo. Os quatro pontos citados por Otto são mudança no processo de análise da rede de reativo para proativo, automatização das defesas, automação inteligente de ameaças e um tratamento de SOC como um serviço em nuvem. Percebemos que com o estudo das melhorias que devem apresentar a unidade SOC, estariam em maior conformidade com a LGPD, pois solucionaria a maioria dos problemas de vulnerabilidades evitando assim ataques e consequentemente o vazamento de informações, bem como mais segurança no processamento de dados.

Diante do que foi exposto e discutido, entendemos que um SOC pode ser uma solução para as organizações estarem em conformidade com a LGPD. As dificuldades de implementação de uma unidade SOC podem ser contornadas com planejamento prévio. Entretanto, destacamos que não deve ser a única solução atuante, pois a unidade SOC também possui a necessidade de evolução. Portanto, ao tratar de novas técnicas de automatização de defesa e computação em nuvem, a nova geração de SOC aborda os problemas e auxilia na questão de altos custos, pois torna a ferramenta mais dinâmica e robusta, dispensando a necessidade de novas soluções onde o SOC não era suficiente para combater aos ataques. Para empresas de médio e pequeno porte, o SOC como serviço em

nuvem é uma forma de popularizar a ferramenta e também solucionar a questão de falta de mão de obra qualificada e complexidade de infraestrutura necessária para a utilização dessa solução.

4 RESULTADOS

A partir dos estudos, das discussões e das análises , juntamente de técnicas como ITIL [26] (*Information Technology Infrastructure Library*) e PMBOK [27] (*Project Management Body Of Knowledge*), conseguimos identificar dois pontos importantes. O primeiro ponto demonstra que o nível de maturidade da segurança da informação de uma empresa determina sua conformidade com a LGPD e o segundo ponto reforça a ideia que ainda há uma lacuna entre o estágio de adequação a LGPD no âmbito de segurança da informação e as organizações. A falta de profissionais capacitados e também a baixa popularização do SOC reforçam a necessidade da elaboração de um plano que mude não somente a parte de tecnologia, mas também a cultura organizacional. Conscientizar os clientes de como proceder com seus dados pessoais também é uma tarefa a ser pensada. Portanto, elaboramos uma escalabilidade de conformidade da LGPD e um plano de implantação de segurança, respectivamente Figura 13 e Figura 14, o qual é regido por técnicas apresentadas no estudo, que possa ser amplamente difundido e capaz contemplar principalmente pequenas e médias empresas, para que estejam em conformidade com a LGPD.

4.1 Nível de Conformidade com a LGPD baseado no nível de segurança da informação de uma empresa

Sabendo que grande parte da LGPD se refere ao tratamento dos dados pessoais, é de suma importância que a equipe responsável pela segurança desses dados esteja alinhada ao regimento brasileiro.

Conforme mostrado na Figura 13, podemos observar que é possível identificar em qual estágio de segurança a empresa se encontra. Por exemplo, supondo que a empresa está na fase de Perímetro e deseja melhorar o seu nível de adequação a LGPD, para alcançar a evolução desejada é necessário alcançar a fase de Prevenção, implementando ferramentas que previnem o ataque como antivírus nas máquinas, IPS, dentre outros. Da mesma forma esta regra é aplicada para qualquer estágio de segurança que demonstra o estado atual e o estado desejado.

Tendo em vista esta constatação e as análises de cenários realizadas na seção anterior, concluímos que o nível de conformidade com a LGPD nos artigos 6°, 9°, 46°, 48° e 50° de uma empresa está diretamente relacionado ao nível de segurança aplicado, ou

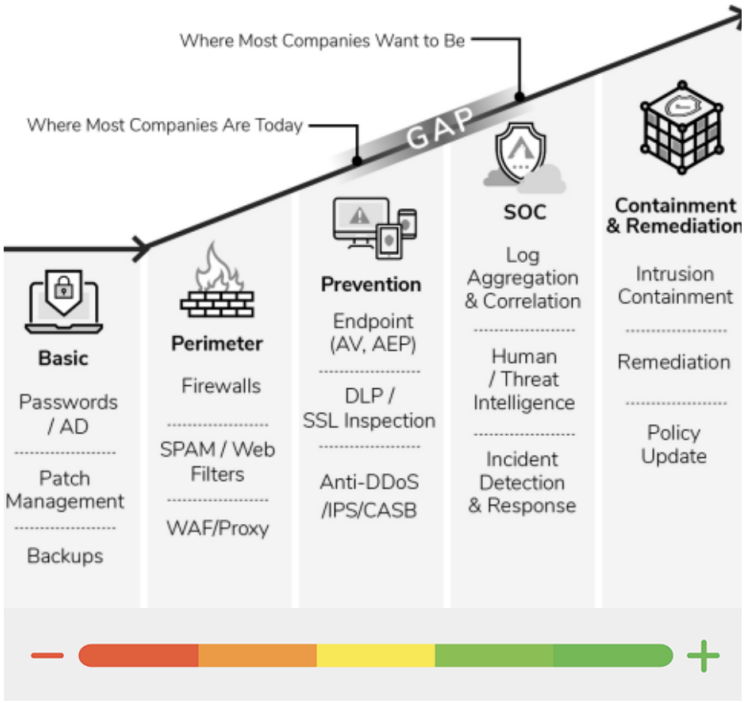

Figura 13: Nível de Conformidade com a LGPD baseado no Nível de Segurança da Informação de uma empresa. Fonte: Autores, adaptado de [1].

seja, quanto mais uma empresa aplica técnicas e ferramentas de defesa mais próxima ela estará da conformidade com a LGPD. Também é importante salientar que mesmo após a implementação do SOC, também existem níveis de SOC que são medidos através das aplicações definidas pela ferramenta. Logo, quanto mais aplicações e maturidade uma implementação SOC tiver, mais ela estará em conformidade com a LGPD.

4.2 Plano de Segurança Organizacional (PSO)

4.2.1 Entendimento do negócio

Cada empresa necessita de uma avaliação que identifique os pontos fortes e fracos, para que seja capaz de direcionar seus investimentos e distribuí-los da melhor forma possível. Para identificar os pontos fortes e fracos, devem ser realizadas análises dos recursos internos, da experiência no mercado, dos ativos tangíveis (maquinário, capital, ferramental, etc), daquilo que a empresa realiza de forma eficiente e aquilo que precisa melhorar, dos recursos humanos e verificação da estratégia da empresa para alcance dos seus objetivos. Nessa parte do plano é aconselhável utilizar uma ferramenta gerencial que

examina o ambiente interno e externo da organização.

É necessário também a identificação de quais dados pessoais serão tratados e seu fluxo dentro da organização. A partir dessa identificação, é fundamental que sejam definidas áreas e restrição de acesso para esses dados. Por exemplo, em um setor de recursos humanos os dados tratados serão dos próprios membros da organização, enquanto no setor de vendas os dados tratados serão do público externo.

Após uma análise completa, é possível que a empresa desenvolva novas estratégias para uma organização a curto, médio e longo prazo. Portanto, é fundamental que esse primeiro passo do plano seja feito com cautela e que percorra todos os pormenores da empresa.

4.2.2 Recursos humanos

No momento em que a organização já entende que realizou uma análise organizacional completa, é de suma importância capacitar os funcionários, conscientizando-os sobre como proceder. Para a empresa no geral, podem ser realizadas palestras internas mostrando a importância do cuidado na troca de informações e a forma correta de manuseio. Para áreas específicas, como recursos humanos e a área de tecnologia, onde existe o contato direto com dados sensíveis, é necessário uma capacitação mais robusta, com cursos internos e externos que geram certificados, comprovando que a empresa está apta a realizar tais atividades. Para essas áreas específicas deve ser realizada uma monitoração constante das atividades e alocados coordenadores responsáveis pela supervisão de pessoal.

Outro ponto de atenção é a figura do controlador de dados, responsável por decisões referentes ao tratamento de dados pessoais. Portanto, é necessário que cada empresa possua um controlador ou um grupo que será atribuído a essas tarefas.

4.2.3 Recursos materiais e investimentos

Após identificar os pontos fortes e fracos e alocar os responsáveis para cada atividade, é necessário que haja ferramental e investimento suficiente para atender as demandas da LGPD. Para tal, serão elencados alguns pontos que facilitam na estruturação empresarial para adequação da norma.

- Políticas de segurança: As políticas de segurança têm por objetivo estabelecer protocolos a serem seguidos dentro de uma organização, de modo a proteger as informações. Definir ferramentas, tipos de acesso, fluxo de informação e medidas a serem tomadas em caso de incidentes fazem parte dessas políticas.

- SOC: Uma estrutura SOC surge como ferramenta de segurança e, é capaz de cruzar dados de eventos gerados nos recursos de segurança da organização como firewalls, IPs e antivírus, possibilitando monitoramento de incidentes como detecção das tentativas de invasão. Devido aos altos custos demandados por uma estrutura de SOC, nem todas empresas têm aporte financeiro para possuir essa infraestrutura. Com o avanço da tecnologia de computação em nuvem, cada vez mais empresas estão aderindo ao contrato com terceiros, seja utilizando o SOC-as-a-service ou terceirizando a ferramenta com empresas especializadas. Portanto, é possível realizar a compra do serviço de segurança, gerando uma redução no investimento realizado e também a não necessidade de manter equipes responsáveis pelo combate de ataques e monitoração de incidentes.

- Medidas de governança: As medidas de governança são responsáveis pela gestão empresarial e por reger boas práticas. Como princípios para a elaboração dessas medidas, temos a equidade, prestação de contas (auditoria), transparência, responsabilidade corporativa, redução de custos e valorização da imagem institucional. Esses fatores são de suma importância, pois garantem que a LGPD está sendo cumprida pela empresa.

- Análise contínua: Para uma melhor performance no tráfego de dados da empresa, é necessário realizar sempre uma avaliação de qualidade no processo. Para tal análise aconselha utilizar o ciclo PDCA (plan-do-check-act) que tem como princípio a melhoria contínua dos serviços. Além dessa análise contínua da empresa como um todo, o SOC é favorecido com uma análise contínua na rede devido a sua busca interna por brechas e resolução dessas brechas para o menor número de ataques cibernéticos.

4.2.4 Transparência

Dentro de todo o plano, um fator importante para a comunicação da empresa é a transparência. A comunicação interna da empresa deve se dar de forma a alcançar todos os funcionários e que todos eles possuam um entendimento do proceder empresarial. Para a comunicação externa, a empresa deve estar sempre alinhada com sua missão, explicando de forma clara quais são as atividades realizadas visando a experiência satisfatória do cliente, bem como o total entendimento do processo pelo contratante. Outro ponto a ser citado é a adequação dos documentos e contratos que envolvam dados pessoais. É importante que estes sejam sempre redigidos de forma a contemplar todas as exigências da lei, não deixando nada acordado de forma verbal e sempre mantendo a transparência em toda a negociação.

4.2.5 Revisão e adequação

É importante salientar que o plano está sujeito a alterações de acordo com as necessidades de cada organização. Portanto, revisar os processos se faz necessário para adequação das atividades, buscando sempre o ponto de convergência entre a qualidade e a entrega do serviço. Essa análise tem como princípio a autogestão da empresa para que haja uma maturidade de identificar os pontos fortes e fracos e estar em constante melhoria.

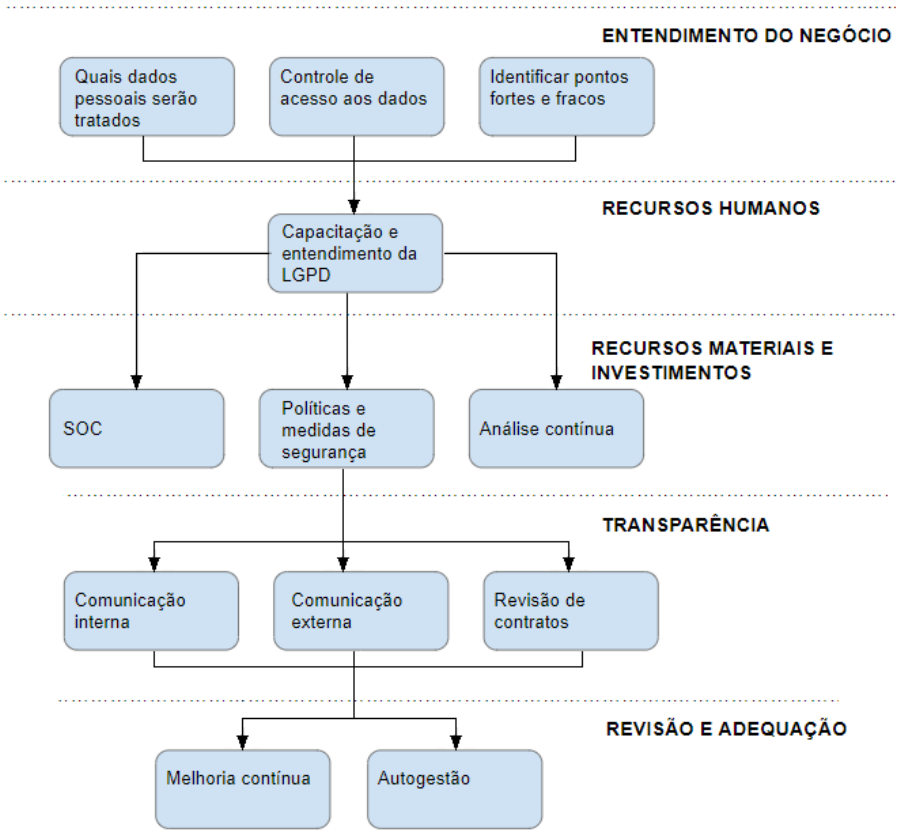

Figura 14: Fluxograma Plano de Segurança Organizacional.

5 CONCLUSÃO

O objetivo da presente pesquisa era ter um melhor entendimento do atual cenário da regulamentação de proteção de dados, de modo que fosse possível compreender as atuais necessidades e propor soluções a partir de ferramentas e tecnologias de segurança da informação. Identificamos que a lei brasileira surgiu em resposta ao regulamento europeu e que suas principais dificuldades na implementação se dão por fatores como cultura interna das organizações, menor rigidez nas penalidades e baixos investimentos no setor de segurança. Além de todas essas dificuldades a sanção da lei ainda é recente, julgando assim necessário maior tempo de adaptação por parte das empresas brasileiras.

Enquanto a LGPD visa a proteção dos dados, as tecnologias utilizadas visam maior efetividade no cumprimento da lei. Nesse contexto, o estudo foca na utilização do SOC como solução. Apesar de ser uma ferramenta indispensável na segurança da informação de uma empresa, destacamos que o SOC não deve ser a única solução atuante, já que ainda possui brechas a serem sanadas. Por ser uma solução de alto custo, é necessário que o uso de SOC seja popularizado. Estudos de novas gerações do SOC já estão sendo feitos e apresentam abordagens que tem como foco a computação em nuvem e a terceirização desses serviços.

A partir dos resultados obtidos neste estudo, percebemos que a falta de profissionais capacitados e também a baixa popularização do SOC reforçam a necessidade de mudança não somente na parte de tecnologia, mas também na cultura organizacional das empresas. Desse modo, houve um entendimento que era necessário elaborar um plano de ação, voltado principalmente para pequenas e médias empresas, capaz de auxiliá-las na maior parte dos aspectos empresariais para que houvesse adequação no artigos referentes à segurança da informação na LGPD. Assim, o objetivo vai além de um estudo para o SOC como solução, contemplando também uma solução para as demais dificuldades encontradas na pesquisa.

Dada a visão geral do cenário atual, percebemos que, mesmo que a passos curtos, há um avanço das empresas e da população com relação ao conhecimento da LGPD. Portanto, refletindo os resultados de curto prazo apresentados pela lei, entendemos que mais estudos são necessários para avaliar a efetividade da lei a médio e longo prazo.

Bibliografia

[1] Crystal Bedell e Mark Bouchard. Definitive Guide to SOC-as-a-Service: The essential elements of advanced threat detection and response. 1ª ed. CyberEdge Group. 2018

[2] GDPR. General Data Protection Regulation (GDPR) [Internet]. General Data Protection Regulation (GDPR). 2018.. Disponível em https://gdpr-info.eu/, Acesso em: Abr. 06, 2022.

[3] L12965 [Internet]. Planalto.gov.br. 2020.. [Internet]. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm, Acesso em: Abr. 06, 2022.

[4] L13709 [Internet]. Planalto.gov.br. 2020.. Disponível em: http://http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm, Acesso em: Abr. 06, 2022.

[5] Veja como ataques de ransomware podem atingir empresas [Internet]. Folha de S.Paulo. 2022. Disponível em https://www1.folha.uol.com.br/mercado/2022/03/veja-como-ataques-de-ransomware-podem-atingir-empresas.shtml, Acesso em: Abr. 06, 2022.

[6] GIL, Antonio Carlos. Como Elaborar Projetos de Pesquisa. 4ª ed. São Paulo: Editora Atlas S.A. 2002

[7] MACHADO, J. M. S. A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados. Revista da AJURIS, v. 41, n. 134, 2014. Disponível em http://www.ajuris.org.br/OJS2/index.php/REVAJURIS/article/view/206, Acesso em: Abr. 06, 2022.

[8] Kalyanpur N, Newman A. Washington Post [Internet]. Analysis — Today, a new E.U. law transforms privacy rights for everyone. Without Edward Snowden, it might never have happened; 25 maio 2018 [citado 6 abr 2022]. Disponível em https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/25/today-a-new-eu-law-tr
Acesso em: Abr. 06, 2022.

[9] GDPR Enforcement Tracker - list of GDPR fines [Internet]. GDPR Enforcement Tracker - list of GDPR fines; Disponível em: https://www.enforcementtracker.com/. Acesso em Abr. 06, 2022.

[10] LOPES, Isabel Maria; GUARDA, Teresa; OLIVEIRA, Pedro. Implementation of ISO 27001 standards as GDPR compliance facilitator. Journal of information systems engineering management, v. 4, n. 2, p. 1-8, 2019.

[11] IMRICHOVÁ, Andrea. GDPR impact on Information Security Incident detection and response.

[12] WOLFF, Josephine; ATALLAH, Nicole. Early GDPR penalties: Analysis of implementation and fines through may 2020. Journal of Information Policy, v. 11, n. 1, p. 63-103, 2021.

[13] Rosemain M. U.S. [Internet]. France fines Google $57 million for European privacy rule breach; 21 jan 2019 Disponível em: https://www.reuters.com/article/us-google-privacy-france-idUSKCN1PF208 Acesso em Abr. 06, 2022.

[14] Dalesio E. Luxembourg Times [Internet]. Luxembourg slaps record €750 million fine on Amazon; 30 jul 2021. Disponível em: https://www.luxtimes.lu/en/business-finance/luxembourg-slaps-record-750-million-fir Acesso em Abr. 06, 2022.

[15] Taylor C. The Irish Times [Internet]. Facebook parent Meta fined €17m by Irish Data Protection Commission; 15 mar 2022 [citado 6 abr 2022]. Disponível em: https://www.irishtimes.com/business/technology/facebook-parent-meta-fined-17m-by-ir 4827584 Acesso em: Abr. 06, 2022.

[16] ERICKSON, Abigayle. Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD. Brook. J. Int'l L., v. 44, p. 859, 2018.

[17] FERREIRA, Lamara; OKANO, Marcelo T. Um panorama da implementação da LGPD no Brasil: uma pesquisa exploratória com 216 profissionais.

[18] Portal do Sebrae SC [Internet]. Panorama LGPD em Santa Catarina - Portal do Sebrae SC. Disponível em: https://www.sebrae-sc.com.br/panorama-lgpd-em-santa-catarina/ Acesso em Abr. 08, 2022.

[19] G1 [Internet]. Cyrela é multada em R$ 10 mil por infração à Lei Geral de Proteção de Dados. Disponível em: https://g1.globo.com/economia/noticia/2020/09/30/cyrela-e-multada-em-r-10-mil-por-i ghtml Acesso em Abr. 08, 2022.

[20] CNN Brasil [Internet]. Justiça reverte decisão e inocenta Cyrela em 1° caso da lei de proteção de dados — CNN Brasil. Disponível em: https://www.cnnbrasil.com.br/business/justica-reverte-decisao-e-inocenta-cyrela-em- Acesso em: Abr. 08, 2022.

[21] ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Tecnologia da informação – Técnicas de Segurança – Código de prática para gestão de segurança da informação. ABNT NBR ISO/IEC n° 17.799:2005, de 30/09/2005.

[22] Ayman El Aassal, Shahryar Baki, Avisha Das, and Rakesh M. Verma. 2019. An In-Depth Benchmarking Evaluation of Phishing Detection Research for Security Needs, 2019

[23] MOHURLE, Savita; PATIL, Manisha. A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, v. 8, n. 5, p. 1938-1940, 2017.

[24] VIELBERTH, Manfred et al. Security operations center: A systematic study and open challenges. IEEE Access, v. 8, p. 227756-227779, 2020.

[25] LINDSTRÖM, Otto. Next Generation Security Operations Center. 2018.

[26] CESTARI FILHO, F. ITIL: Information Technology Infrastructure Library. Rio de Janeiro: RNP/ESR, 2011.

[27] PMI. Um guia do conhecimento em gerenciamento de projetos. Guia PMBOK 6ª.ed - EUA: Projects Management Institute, 2017