UNIVERSIDADE FEEVALE

ÂNDERSON DIONÍZIO BERVANGER

OAS FRAMEWORK - SEGURANÇA DA INFORMAÇÃO COM ADERÊNCIA PARA LGPD E CERTIFICAÇÃO OEA

Novo Hamburgo

2021

ÂNDERSON DIONÍZIO BERVANGER

OAS FRAMEWORK - SEGURANÇA DA INFORMAÇÃO COM ADERÊNCIA PARA LGPD E CERTIFICAÇÃO OEA

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do grau de Bacharel em Sistemas de Informação pela Universidade Feevale

Orientador: Prof. Dr. Paulo Ricardo Muniz Barros

Novo Hamburgo

2021

AGRADECIMENTOS

Gostaria de agradecer a todos os que, de alguma maneira, contribuíram para a realização desse trabalho de conclusão, em especial:

A minha família por sempre estar presente e apoiando meus passos.

A minha namorada, por toda a paciência, motivação e apoio incondicional nesta etapa.

Ao professor Dr. Paulo Ricardo, pelas orientações, empenho e disposição na produção deste trabalho.

A todos amigos que me apoiaram nessa jornada desde o primeiro semestre até a conclusão dessa etapa.

Aos participantes do estudo que de forma espontânea e brilhante contribuíram com o desenvolvimento do trabalho.

Muito obrigado!

RESUMO

Nas últimas décadas ocorreram diversas mudanças nos processos de comércio exterior, desde a maneira em que a carga é transportada até o volume e rapidez das negociações no mundo. Essa mudança pode trazer benefícios, como o crescimento da economia, mas também pode ser uma abertura para ameaças. Programas de segurança e conformidade tem sido desenvolvidos por aduanas pelo mundo para selecionar empresas seguras e permitir um fluxo facilitado. Uma das iniciativas é o Operador Econômico Autorizado (OEA), que certifica empresas que cumpram os critérios de segurança aplicados à cadeia logística. As empresas que desejam essa certificação devem cumprir critérios de elegibilidade, entre eles, critérios de segurança da informação. Ao mesmo tempo em que desenvolveu o programa OEA, o Brasil avançou em sua legislação para ter uma lei que dite as normas para a proteção de dados, lei essa chamada Lei Geral de Proteção de Dados (LGPD). Por serem implementações recentes expostas na sociedade brasileira, existe uma lacuna de conhecimento sobre quais processos podem ser feitos para uma adequação às normas vigentes. Assim, o presente trabalho tem como objetivo propor um *framework* de segurança da informação que auxilie organizações na adequação à Lei Geral de Proteção dos Dados (LGPD) e que tenha aderência com os critérios de elegibilidade exigidos pela certificação de Operador Econômico Autorizado (OEA). A metodologia escolhida para o desenvolvimento do estudo foi o *Design Science Research* (DSR), que é um modelo aceito e válido para o desenvolvimento de artefatos para a ciência da informação.

Palavras-chave: Segurança da informação. LGPD. OEA. Framework.

ABSTRACT

In recent decades, there have been several changes in foreign trade processes, from the way cargo is transported to the volume and speed of negotiations in the world. This shift can bring benefits such as economic growth, but it can also be an opening for threats. Security and compliance programs have been developed by customs around the world to select secure companies and allow for easy flow. One of the initiatives is the Authorized Economic Operator (AEO), which certifies companies that meet the safety criteria applied to the supply chain. Companies seeking this certification must meet eligibility criteria, including information security criteria. At the same time as developing the AEO program, Brazil advanced in its legislation to have a law that sets the standards for data protection, the so-called General Data Protection Regulation (GDPR). As these are recent implementations exposed in Brazilian society, there is a gap in knowledge about which processes can be carried out to adapt to current standards. Thus, this work aims to propose an information security framework that helps organizations in adapting to the General Data Protection Regulation (GDPR) and that meets the eligibility criteria required by the Authorized Economic Operator (AEO) certification. The methodology chosen for the development of the study was Design Science Research (DSR), which is an accepted and valid model for the development of artifacts for information science.

Keywords: Information security. GDPR. AEO. Framework.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE GRÁFICOS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AEO	*Authorized Economic Operator*
ARM	Acordos de Reconhecimento Mútuo
ART	Artigo
CAP	Capítulo
CND	Certidão Negativa de Débitos
COBIT	*Control Objectives for Information and Related Technologies*
DPO	*Data Protection Officer*
DSR	*Design Science Research*
DTE	Domicílio Tributário Eletrônico
ECD	Escrituração Contábil Digital
GDPR	*General Data Protection Regulation*
ID	Identificação
IEC	*International Electrotechnical Commission*
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standardization*
LGPD	Lei Geral de Proteção de Dados
NBR	Norma Brasileira
OAS	Operador Autorizado Seguro
OEA	Operador Econômico Autorizado
OMA	Organização Mundial das Aduanas
PDCA	*Plan-Do-Check-Act*
RFB	Receita Federal Brasileira
SAFE	*Framework of Standards to Secure and Facilitate Trade*
SGPI	Sistema de Gestão da Privacidade
SGSI	Sistema de Gestão de Segurança da Informação
TCC	Trabalho de Conclusão de Curso
TI	Tecnologia da Informação
VPN	*Virtual Private Network*

SUMÁRIO

1 INTRODUÇÃO

No que tange ao ambiente do comércio internacional, RAZUMEY (2014) afirma que nas últimas décadas, houve significativas transformações na maneira como as cargas são transportadas e comercializadas, bem como à rapidez e ao volume dessas transações realizadas em todo o mundo. Ainda segundo RAZUMEY (2014), essas mudanças vistas em conjunto com a pressão do comércio internacional para a minimização da intervenção dos governos, são a causa das autoridades internacionais de aduana estarem dando ênfase maior na facilitação do comércio.

A globalização que o mundo experimenta desde o final do século XX vem provocando um vertiginoso aumento do fluxo de pessoas e mercadorias entre os diversos países, fato que apesar de trazer muitos benefícios, como o crescimento da economia mundial, traz também seu lado negativo: o de ser uma porta de entrada, principalmente, para o terrorismo. (BRASIL, 2018).

Quando observamos o crime organizado internacional, BRASIL (2018) destaca que diversas facções terroristas se aproveitam desse volumoso fluxo comercial para circular mercadorias, ilícitas ou descaminhadas, às margens das fiscalizações aduaneiras, fomentando dessa forma o tráfico de drogas e armas, contrabando, lavagem de dinheiro, entre outras atividades criminosas.

PEREIRA II *et al.* (2018) destaca que os programas de segurança e de conformidade aduaneira têm sido utilizados por várias aduanas do mundo, como forma de selecionar as empresas confiáveis e permitir-lhes trânsito facilitado nas operações de passagem de fronteira.

GARCIA (2018) ressalta a necessidade de os países desenvolverem a participação e operação do comércio exterior, criando relações, acordos e tratados com outros países mais desenvolvidos. Destaca também que este desenvolvimento facilita para que o país se desenvolva em segmentos em que ele próprio não tem recursos, havendo a necessidade de adquirir estes meios de outros países.

MACHADO *et al.* (2015) afirma que dentre as iniciativas que surgiram na última década, destaca-se o Operador Econômico Autorizado (OEA), proposto como um programa de certificação voluntária dos elos da cadeia de suprimentos internacionais. SILVA JUNIOR (2019) destaca que o programa OEA busca estabelecer parcerias entre as aduanas e os intervenientes no comércio exterior (importadores, exportadores, transportadores, armazéns), compartilhando assim as responsabilidades e aumentando a capacidade de fiscalização das atividades aduaneiras, trazendo maior segurança à cadeia de suprimentos internacional.

Segundo o parágrafo 1º do art. 1º da Instrução Normativa da Receita Federal Brasileira nº 1598/2015,

> Entende-se por Operador Econômico Autorizado (OEA) o interveniente em operação de comércio exterior envolvido na movimentação internacional de mercadorias a qualquer título que, mediante o cumprimento voluntário dos critérios de segurança aplicados à cadeia logística ou das obrigações tributárias e aduaneiras, conforme a modalidade de certificação, demonstre atendimento aos níveis de conformidade e confiabilidade exigidos pelo Programa OEA. (BRASIL, 2018, P. 10).

O Programa de Operador Econômico Autorizado (OEA) surgiu com a finalidade de facilitar e tornar mais seguro o comércio mundial por meio da integração e da padronização entre as aduanas e os agentes governamentais, permitindo melhorar o fluxo comercial global. (DE ANDRADE; CASSANO; DE SOUZA, 2018).

Para um interveniente em comércio exterior ser certificado como Operador Econômico Autorizado, é necessário que cumpra os critérios de elegibilidade. BRASIL (2018) afirma que os critérios de elegibilidade são condições que traduzem o grau de confiabilidade dos operadores, requerentes da certificação OEA. É também destacado que os critérios de confiabilidade são dispostos no Art. 15 em conjunto com o item I do anexo II e o bloco II da Instrução Normativa RFB nº 1598/2015:

- Histórico do cumprimento da legislação aduaneira.
- Gestão da informação.
- Solvência financeira.
- Política de recursos humanos.
- Gerenciamento de riscos aduaneiros.

No que tange a Gestão da informação, um dos requisitos dispostos é o requisito da Segurança da Informação. O item 1.2.2.2 do anexo II da instrução Normativa RFB nº 1598/2015 dispõe os itens a serem alcançados para o operador certificado:

- As informações relacionadas com os as operações de comércio exterior devem ser protegidas contra acesso não autorizado.
- Autorizações de acesso a informações devem ser concedidas para cada funcionário individualmente.
- A autenticação de acesso a informações deve ocorrer por meio de senha, com política de renovação definida.

- Deve existir política de segurança da informação, de conhecimento por parte de toda a organização.
- Medidas devem ser adotadas a fim de identificar violações à política de segurança da informação da organização.
- Devem ser previstas medidas disciplinares aplicáveis aos casos de violação à política de segurança da informação.
- As informações relacionadas com as operações de comércio exterior devem ser armazenadas de forma que possibilite sua restauração.

Segundo AGRA (2018), a segurança da informação está diretamente relacionada com a proteção de um conjunto de informações. A necessidade de investir em assegurar as informações não para de crescer. HINTZBERGEN *et al.* (2018) define segurança da informação como a proteção da informação contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar os riscos de negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio.

A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT, 2013).

Vale frisar que tão importante quanto obter a certificação de Operador Econômico Autorizado, a empresa deve obedecer às leis vigentes que abrangem a segurança dos dados que a empresa tem posse. DA ROCHA *et al.* (2019) discorre que, diante dos recentes acontecimentos de uso indevido de dados pessoais, a Lei Geral de Proteção de Dados (LGPD) transmite um passo relevante para o Brasil, as novas regras vão assegurar a privacidade dos brasileiros.

A LGPD, Lei nº 13.709, de 14 de agosto de 2018, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da pessoa natural. (BRASIL, 2020).

Dispostas assim as informações sobre a importância para os intervenientes em comércio exterior de obter a certificação de Operador Econômico Autorizado, é importante notar que a segurança da informação dispõe de um papel crucial no fluxo do comércio exterior visando a segurança das operações nas aduanas e trânsito aduaneiro. Percebe-se hoje

uma lacuna de trabalhos acadêmicos que englobem boas práticas ou políticas de segurança da informação para empresas que querem estar alinhadas com o exigido pela Receita Federal para obtenção da certificação OEA nos termos de segurança da informação.

Também é necessário ressaltar que a Lei Geral de Proteção de Dados trouxe uma nova perspectiva na forma em que as organizações tratam a informação e sua segurança, devendo se adequar na legislação de forma a não sofrer punições perante a justiça brasileira.

Assim, o presente trabalho dispõe da seguinte perspectiva: Quais são os aspectos relevantes em um *framework* de segurança da informação que tenha aderência com a LGPD e com os critérios de elegibilidade exigidos para uma empresa que deseja ser certificada como Operador Econômico Autorizado?

1.1 OBJETIVOS

Na sequência estão expostos os objetivos do trabalho, sendo esses definidos com um objetivo geral e objetivos específicos que irão complementar a ideia proposta para o trabalho.

1.1.1 Objetivo geral

Desenvolver um framework de segurança da informação que auxilie organizações na adequação a Lei Geral de Proteção dos Dados (LGPD) e que tenha aderência com os critérios de elegibilidade exigidos pela certificação de Operador Econômico Autorizado (OEA).

1.1.2 Objetivos específicos

- Desenvolver estudo teórico sobre a certificação Operador Econômico Autorizado (OEA), Lei Geral de Proteção de Dados (LGPD) e demais leis de segurança da informação vigentes no Brasil.
- Elaborar uma pesquisa sobre os frameworks de segurança da informação existentes.
- Elaborar níveis de maturidade do framework criado.
- Realizar avaliação qualitativa do framework com especialistas.
- Coletar e divulgar resultados sobre o framework desenvolvido.

1.2 ESTRUTURA DO TRABALHO

Primeiro, no Capítulo 2, são apresentadas as características relacionadas à metodologia de pesquisa escolhida. No capítulo 3 é apresentada a certificação Operador Econômico Autorizado (OEA), sua história, requisitos, critérios de elegibilidade, certificações, benefícios e adoção no Brasil. No capítulo 4 é destacada a Lei Geral de Proteção de Dados (LGPD), apresentando o caminho que levou o Brasil até a concepção dessa lei, suas principais contribuições, as exigências, os requisitos de segurança da informação e boas práticas de governança. A família de normas da ISO/IEC 27000 é apresentada no capítulo 5, através dos seus requisitos e estruturas. O capítulo 6 é reservado para a explanação sobre o COBIT 5, expondo as vantagens, princípios e modelo de capacidade de processo. A revisão da literatura é abordada no capítulo 7, apresentando trabalhos que são relevantes para o modelo de framework que será apresentado. O capítulo 8 apresenta o artefato desenvolvido, o OAS Framework e seus controles e módulos. O modelo de implementação proposto para o Framework é explicado no capítulo 9. No capítulo 10 são exibidos os resultados do questionário respondido pelos especialistas em comércio exterior e Gestão de TI. Por fim, no capítulo 11 é feita a conclusão do presente trabalho.

2 METODOLOGIA

A metodologia que será utilizada no trabalho será a *Design Science Research* (DSR). Segundo JAPPUR (2014), a DSR busca preencher a falta de uma metodologia para servir de modelo aceito e válido para o desenvolvimento de artefatos para a ciência da informação.

JAPPUR (2014), baseado em PEFFERS *et al.* (2007), elenca as seis atividades da DSR. Estas seis atividades seguem uma sequência nominal ou procedural:

1. **Identificação do problema e motivação:** Buscar frameworks de segurança da informação já existentes, buscar estudos sobre a certificação Operador Econômico Autorizado, sobre a Lei Geral de Proteção de Dados (LGPD) e demais leis da segurança da informação vigentes no Brasil.
2. **Definição dos objetivos:** Buscar frameworks de segurança da informação que auxiliem organizações na adequação a Lei Geral de Proteção dos Dados (LGPD) e que tenham aderência com os critérios de elegibilidade exigidos pela certificação de Operador Econômico Autorizado (OEA).
3. ***Design* e desenvolvimento:** Desenvolver o framework propriamente dito, que seja capaz de ser a base para organizações se adequarem à certificação e as leis brasileiras.
4. **Demonstração:** Apresentar o modelo de framework proposto para gestores que adquiriram a certificação OEA ou buscam adquirir a certificação e adequação as normas brasileiras.
5. **Avaliação:** Realizar uma avaliação qualitativa com os gestores sobre a aderência do framework em suas organizações.
6. **Comunicação:** Apresentação final do TCC e postagem do trabalho para consultas posteriores na internet.

Para o desenvolvimento do Framework proposto a natureza da pesquisa é Pesquisa Aplicada, de caráter exploratório, apoiada na legislação Brasileira referente a proteção de dados pessoais e comércio exterior, nas normas da família ISO 27000, norma COBIT e frameworks de Segurança da Informação diversos.

Segundo PRODANOV e FREITAS (2013), a pesquisa aplicada busca gerar conhecimentos para a aplicação prática dirigidos à solução de problemas específicos. Os

autores explicam também que a pesquisa de caráter exploratório possui planejamento flexível, permitindo o estudo do tema sob diversos ângulos e aspectos.

É importante frisar também a importância do artigo nº 46 da LGPD para a pesquisa, o artigo cita que:

> 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 (BRASIL. Lei nº 13709, art. nº 46).

Segundo DA ROCHA *et al.* (2019), todas as empresas não importando o seu porte devem utilizar meios para se adequar a LGPD, tendo assim o artigo nº 46 validado a utilização da norma ISO 27001 como controle para requisitos da lei, mas não se limitando somente a essa normativa.

3 OEA

Ao se referir ao processo de globalização, SILVA JUNIOR (2019) avalia que houve um exponencial aumento do fluxo de pessoas, serviços e mercadorias entre os países, sendo que apesar de trazer benefícios, tais como o crescimento da economia mundial, também tem um lado negativo, que é poder ser usado como camuflagem para atividades ilegais, especialmente o terrorismo.

De acordo com LEOCE e MORINI (2011, *apud* DE ANDRADE; CASSANO; DE SOUZA, 2018) o aumento do comércio internacional impossibilitou a conferência física de todos os embarques, tornando-se necessário o desenvolvimento de alternativas que permitissem maior agilidade às aduanas.

PEREIRA, MORINI e GREGORACCI (2014) destacam que, principalmente após os ataques terroristas de 11 de setembro de 2001, as novas responsabilidades da aduana devem incorporar medidas de segurança que sejam acessíveis e promovam o comércio entre países.

GORDHAN (2007) destaca que a Organização Mundial das Aduanas (OMA), uma organização intergovernamental que representa 170 administrações aduaneiras, através do seu conselho, em uma das suas sessões de junho de 2005, adotou o *Framework of Standards to Secure and Facilitate Trade (SAFE)*.

Ainda segundo GORDHAN (2007), o principal objetivo do *SAFE Framework* é estabelecer padrões que forneçam à cadeia de abastecimento segurança e facilitação global para promover certeza e previsibilidade. Para TWEDDLE (2008), o principal objetivo do *SAFE Framework* é assegurar e facilitar o comércio em nível global por meio do estabelecimento de arranjos cooperativos entre diversas aduanas, entre o comércio e outras agências dos governos, a fim de promover um melhor fluxo de cargas por meio do comércio internacional seguro.

Entre as recomendações do *SAFE Framework*, PEREIRA, MORINI e GREGORACCI (2014) apontam:

a) Sistemas eletrônicos sejam utilizados para maior vigilância e agilidade do desembaraço aduaneiro.
b) Sejam empregadas técnicas de gerenciamento de risco ao selecionar bens para a inspeção.
c) Haja cooperação entre as aduanas de outros países.
d) Seja assegurado que as leis e regulações aduaneiras sejam transparentes e acessíveis ao público.

BRASIL (2018) apresenta os três pilares nos quais o S*AFE Framework* é sustentado:

1) **ADUANA-ADUANA**: Maior cooperação entre as aduanas dos países, a fim de otimizar a facilitação e a segurança das cadeias logísticas internacionais. Um exemplo de cooperação seria o intercâmbio de informações entre as aduanas antes da chegada da carga no país de destino, de modo a possibilitar o gerenciamento do risco e concentração dos esforços nas cargas com maior nível de risco.
2) **ADUANA-EMPRESA:** Parceria entre a alfândega e o setor privado, objetivando a construção conjunta de políticas de segurança à cadeia logística. É dentro deste pilar que aparece a figura do Operador Econômico Autorizado (OEA).
3) **ADUANA-OUTRAS AGÊNCIAS DO ESTADO**: Parceria entre a Aduana e outras agências de Estado Envolvidas no comércio internacional de forma a garantir uma resposta rápida do Estado aos desafios da segurança da cadeia logística e ao mesmo tempo, evitar duplicidades de requerimentos e inspeções, simplificar e padronizar os processos de forma a facilitar o comércio internacional.

Ainda sobre o conceito de OEA, DE ANDRADE; CASSANO; DE SOUZA (2018) afirmam que um OEA é uma parte envolvida no movimento internacional de cargas, em qualquer função, que tenha sido aprovado por uma ou em nome de uma administração aduaneira nacional, a partir do momento em que se adequou aos quesitos estabelecidos pela Organização Mundial das Aduanas, podendo se beneficiar do reconhecimento mútuo de seu *status* com outras aduanas do mundo.

Citando a edição de 2017 do documento chamado *Compendium of Authorized Economic Operator Programmes* da Organização Mundial das Aduanas, BRASIL (2018) informa que há 73 Programas de OEA implementados no mundo e outros 17 em desenvolvimento.

O Programa Brasileiro de OEA é normatizado pela Instrução Normativa da Receita Federal do Brasil nº 1598 de 09 de dezembro de 2015. Segundo o artigo 3º da Instrução Normativa RFB nº 1598, são objetivos do Programa OEA:

- Proporcionar maior agilidade e previsibilidade no fluxo do comércio internacional.
- Buscar a adesão crescente de operadores econômicos, inclusive pequenas e médias empresas.

- Incrementar a gestão do risco das operações aduaneiras.
- Firmar Acordos de Reconhecimento Mútuo (ARM) que atendam aos interesses do Brasil.
- Implementar processos de trabalho que visem a modernização da Aduana.
- Intensificar a harmonização dos processos de trabalho com outros órgãos regulatórios do comércio exterior.
- Elevar o nível de confiança no relacionamento entre operadores econômicos, a sociedade e a Secretaria da Receita Federal do Brasil.
- Priorizar as ações da Aduana com foco nos operadores de comércio exterior de alto risco ou risco desconhecido.
- Considerar a implementação de outros padrões que contribuam com a segurança da cadeia logística.

A Instrução Normativa RFB nº 1598 possibilita a certificação dos intervenientes nas seguintes modalidades:

- **OEA-SEGURANÇA (OEA-S)**, com base em critérios de segurança aplicados à cadeia logística no fluxo das operações de comércio exterior.
- **OEA-CONFORMIDADE (OEA-C)** com base em critérios de cumprimento das obrigações tributárias e aduaneiras, e que apresenta níveis diferenciados quanto aos critérios exigidos e aos benefícios concedidos: OEA-C Nível 1 e OEA-C Nível 2.

Os intervenientes devem escolher a certificação OEA conforme o disposto no quadro abaixo:

Quadro 1 – Intervenientes por modalidade de certificação OEA

Intervenientes Certificáveis	**OEA-S**	**OEA-C1**	**OEA-C2**
Importador	X	X	X
Exportador	X	X	X
Transportador	X		
Agente de carga	X		
Depositário de mercadoria em recinto alfandegado	X		

Operador Portuário e Aeroportuário	X		
Recinto Esp. Despacho Aduaneiro de Expo - Redex	X		

Fonte: Adaptado de BRASIL (2018, p. 28).

O artigo 9º da Instrução Normativa RFB nº 1598/2015 lista os benefícios de caráter geral, que se aplicam a todas as modalidades de certificação OEA. No quadro 2 são listados os benefícios de caráter geral em relação as modalidades de certificação:

Quadro 2 – Benefícios de caráter geral

Benefícios OEA	**OEA-S**	**OEA-C1**	**OEA-C2**
Publicidade no site da RFB	X	X	X
Utilização da logomarca "AEO"	X	X	X
Ponto de contato na RFB	X	X	X
Prioridade na análise em outras modalidades OEA	X	X	X
Benefícios concedidos pelas Aduanas Estrangeiras	X	X	X
Participação no Fórum Consultivo	X	X	X
Dispensa de exigências já cumpridas no OEA	X	X	X
Participação em Seminários e	X	X	X

treinamentos			

Fonte: Adaptado de BRASIL (2018, p. 30).

Sobre os benefícios específicos de cada modalidade de certificação, o artigo 10º da Instrução Normativa RFB nº 1598/2015 lista os benefícios para o interveniente certificado na modalidade OEA-S. O quadro abaixo relaciona os benefícios da OEA-S em relação as outras modalidades.

Quadro 3 – Benefícios Da OEA-S

Benefícios OEA	OEA-S	OEA-C1	OEA-C2
Parametrização imediata das declarações de exportação (DE)	X		
Redução do percentual de canais na exportação	X		
Prioridade de conferência das declarações selecionadas (DE)	X		
Dispensa de garantia no trânsito aduaneiro	X		
Acesso prioritário a transportador OEA em recintos aduaneiros	X		

Fonte: Adaptado de BRASIL (2018, p. 31).

O artigo 11º e 12º da Instrução Normativa RFB nº 1598/2015 determinam os benefícios para os importadores certificados na modalidade OEA-C Nível 1 e Nível 2. O quadro 4 ilustra os benefícios para os importadores na modalidade OEA-C Nível 1 e Nível 2:

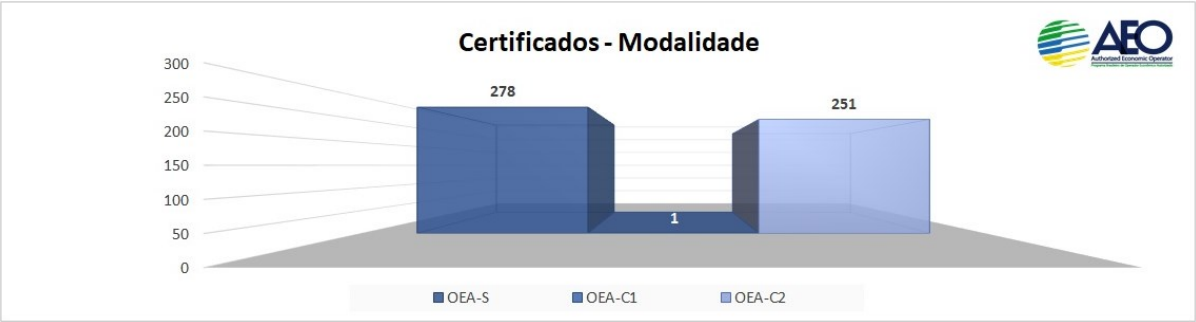
Quadro 4 – Benefícios da OEA-C1 e OEA-C2

Benefícios OEA	OEA-S	OEA-C1	OEA-C2
Resposta à consulta de classificação fiscal em até 40 dias		X	X
Dispensa garantia na Admissão temporária		X	X
Carga Pátio por 24h no modal aéreo		X	X
Parametrização imediata das declarações de importação (DI)			X
Redução do percentual de canais na importação			X
Prioridade de conferência das declarações selecionadas (DI)			X
Despacho sobre águas OEA (portaria COANA nº 85/2017)			X
Canal verde na Admissão Temporária			X

Fonte: Adaptado de BRASIL (2018, p. 32).

De acordo com a Receita Federal (2021), em 31 de março de 2021 o Programa OEA havia emitido 530 certificados e restavam 137 requerimentos em análise. Dos 530 certificados emitidos, 278 são certificados OEA-S, 01 certificado OEA-C1 e 251 certificados OEA-C2. A figura abaixo nos mostra a quantidade de certificados emitidos por modalidade:

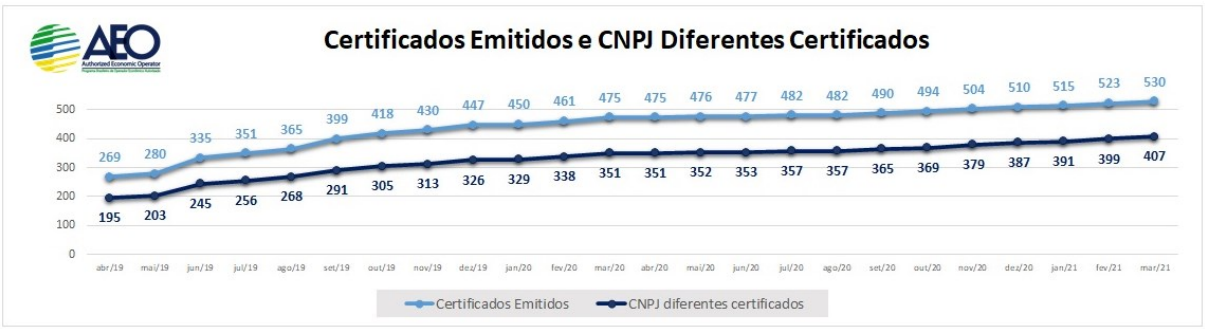
Figura 1 – Certificados emitidos conforme modalidade



Fonte: Receita Federal (2021).

No período correspondente de abril de 2019 até março de 2021, foram emitidas 261 certificações. Devido a pandemia de Covid-19, o processo de certificação em 2020 e 2021 ficou prejudicado em comparação com o de 2019, pois as validações físicas que são fundamentais na análise da modalidade OEA-S foram suspensas. A Figura 2 mostra a evolução de certificados emitidos e CNPJ diferentes certificados. (RECEITA FEDERAL, 2021).

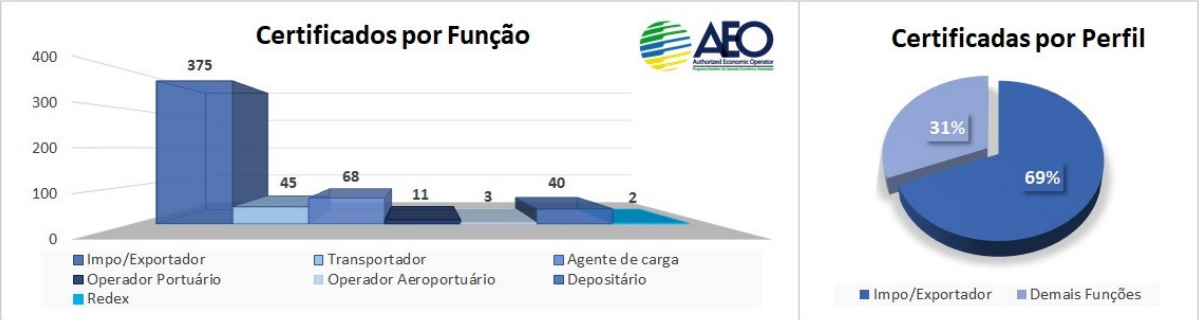
Figura 2 – Certificados Emitidos e CNPJ Diferentes Certificados



Fonte: Receita Federal (2021).

A Receita Federal (2021) também destaca que alguns dos certificados emitidos possuem mais de uma função na cadeia logística certificada. Assim, as 530 certificações emitidas até a publicação da estatística, autorizam 544 funções distribuídas conforme imagem abaixo, ilustrando os certificados por função e certificados por perfil:

Figura 3 – Certificados por Função e Certificados por Perfil



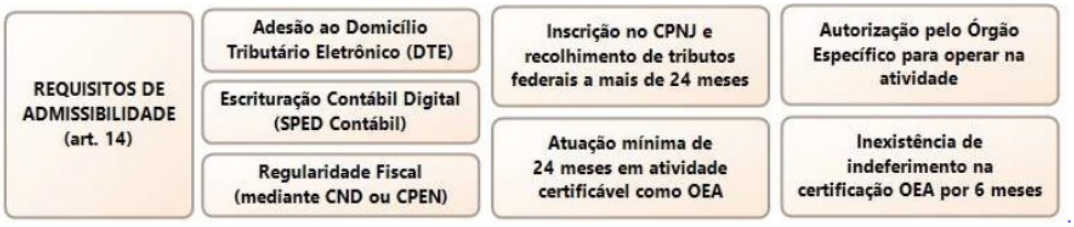
Fonte: Receita Federal (2021).

Segundo BRASIL (2018), o interveniente que deseja obter a certificação de Operador Econômico Autorizado deve cumprir quesitos de admissibilidade que estão dispostos nos oito incisos do artigo nº 14 da instrução normativa RFB nº 1598/2015, onde é avaliado se o operador está apto a participar do processo de certificação:

1. Adesão ao Domicílio Tributário Eletrônico (DTE);
2. Adesão à Escrituração Contábil Digital (ECD);
3. Comprovação de Regularidade Fiscal, por meio de Certidão Negativa de Débitos Relativos à Créditos Tributários Federais e à Dívida Ativa da União (CND), nos termos da Portaria Conjunta RFB/PGFN nº 1751/2014;
4. Inscrição no CNPJ e recolhimento de tributos federais há mais de 24 meses;
5. Atuação como interveniente em atividade passível de certificação OEA por, no mínimo, 24 meses;
6. Autorização para o requerente operar em sua área de atuação, nos termos estabelecidos pelo órgão de controle específico quando for o caso;
7. Inexistência de indeferimento de pedido de certificação ao Programa OEA nos últimos 6 meses.

Segue resumo dos quesitos de admissibilidade na figura 4 abaixo:

Figura 4 – Requisitos de Admissibilidade do Programa Brasileiro de OEA



Fonte: BRASIL (2018, p. 41).

Para um interveniente em comércio exterior ser certificado como Operador Econômico Autorizado, é necessário que cumpra os critérios de elegibilidade. BRASIL (2018) afirma que os critérios de elegibilidade são condições que traduzem o grau de confiabilidade dos operadores, requerentes da certificação OEA. É também destacado que os critérios de confiabilidade são dispostos no art.15 em conjunto com o item I do anexo II e o bloco II da Instrução Normativa RFB nº 1598/2015. A figura 5 ilustra os critérios de elegibilidade do Programa Brasileiro de OEA:

- Histórico do cumprimento da legislação aduaneira: Evitar a reincidência de infração à legislação aduaneira.
- Gestão da informação: Assegurar a disponibilidade e exatidão de registros comerciais relacionados com as operações de comércio exterior. Assegurar exatidão de informações de interesse aduaneiro declaradas.
- Solvência financeira: Manter e aperfeiçoar todos os controles ligados aos critérios do Programa OEA.
- Política de recursos humanos: Evitar admissão ou manutenção de pessoal que represente ameaça à cadeia logística ou à conformidade aduaneira.
- Gerenciamento de riscos aduaneiros: Identificar, analisar, priorizar, tratar e monitorar eventos capazes de afetar os objetivos relacionados com os critérios do programa OEA.

Figura 5 – Critérios de Elegibilidade do Programa Brasileiro de OEA

Fonte: BRASIL (2018, p. 45).

No que tange a Gestão da informação, um dos requisitos dispostos é o requisito da Segurança da Informação. O item 1.2.2.2 do anexo II da instrução Normativa RFB nº 1598/2015 dispõe os itens a serem alcançados para o operador certificado:

- Item 1.2.2.2.A: As informações relacionadas com os as operações de comércio exterior devem ser protegidas contra acesso não autorizado.

- Item 1.2.2.2.B: Autorizações de acesso a informações devem ser concedidas para cada funcionário individualmente.
- Item 1.2.2.2.C: A autenticação de acesso a informações deve ocorrer por meio de senha, com política de renovação definida.
- Item 1.2.2.2.D: Deve existir política de segurança da informação, de conhecimento por parte de toda a organização.
- Item 1.2.2.2.E: Medidas devem ser adotadas a fim de identificar violações à política de segurança da informação da organização.
- Item 1.2.2.2.F: Devem ser previstas medidas disciplinares aplicáveis aos casos de violação à política de segurança da informação.
- Item 1.2.2.2.G: As informações relacionadas com as operações de comércio exterior devem ser armazenadas de forma que possibilite sua restauração.

Conforme exposto acima, é de grande importância que o Brasil tenha um programa que facilite o comércio para intervenientes autorizados, garantindo agilidade no processo e principalmente a segurança nos processos do comércio exterior. A segurança da informação é parte fundamental do processo de importação e exportação, sendo fator chave para garantir a segurança do comércio, empresas, países e cidadãos do mundo.

É importante frisar que, além de contemplar os requisitos de segurança da informação para a certificação OEA, o interveniente também deve estar de acordo com as demais leis do país. No cenário atual, a lei que vem mobilizando esforços de todas as empresas para buscar a adequação devida é a Lei Geral de Proteção de Dados (LGPD), que será tratada no próximo capítulo.

4 LGPD

Sobre a proteção de dados pessoais, IRAMINA (2020) discorre que em uma sociedade cada vez mais informatizada, na qual o fluxo de dados se tornou um componente crucial para o comércio e para as comunicações e as interações sociais, a proteção de dados pessoais passou a ser uma preocupação para grande parte dos países como Coréia do Sul, Chile, Tailândia, Índia, Indonésia e Brasil, tendo esses adotado novas regras de proteção de dados ou modernizado as que já tinham.

BATISTA; OBREGÓN (2020) afirmam que a sociedade atual se encontra na denominada Era de Dados, também denominada Big Data, expressão usada para se referir à colossal quantidade de dados coletados dos usuários da web que interagem por meios virtuais, com ou sem o seu consentimento, e utilizados das maneiras mais diversas, seja por entes privados ou por entes públicos.

BATISTA; OBREGÓN (2020) também avaliam que mediante a utilização dos dados de usuários da web com e sem consentimento, fez-se necessária a criação de mecanismos para a proteção da privacidade dos cidadãos que utilizam a internet. Os autores citam a elaboração do Marco Civil da internet no Brasil e, posteriormente, da Lei Geral de Proteção de Dados (LGPD).

VIEIRA (2019) mostra que no ordenamento jurídico brasileiro, a proteção de dados foi inicialmente admitida como princípio relativo ao uso da internet, expressamente consagrado pela Lei Nº 12.965, o Marco Civil da Internet. A lei estabeleceu em seu artigo 3º, inciso III, a elaboração específica para a proteção de dados, o que só aconteceu na data em que a LGPD foi aprovada.

Para LORENZON (2021), apesar de não ter foco no assunto de dados pessoais, o Marco Civil da Internet foi pioneiro na delimitação de direitos e deveres para os usuários na Internet, além de estabelecer diretrizes para a atuação do governo brasileiro perante o assunto.

BATISTA; OBREGÓN (2020) destacam o capítulo II da lei do Marco Civil da Internet, que trata dos direitos e garantias dos usuários, assegura-se aos usuários diversos direitos, dentre eles a inviolabilidade das comunicações privadas (art. 7º, II), bem como o sigilo de suas comunicações privadas armazenadas (art. 7º, III). Destacam também o inciso VIII do art 7º da mesma lei, que assegura aos usuários informações claras sobre como seus dados estão sendo utilizados, desde a coleta, uso, armazenamento, tratamento, até a proteção de dados.

Para BATISTA; OBREGÓN (2020) o Marco Civil da Internet foi o nascimento de uma tentativa de regulamentar um quadro de incertezas dos usuários da internet no que diz respeito à privacidade, sendo que em muitas vezes os usuários não sabem como as informações pessoais depositadas na rede estão sendo utilizadas ou compartilhadas.

LORENZON (2021) destaca que o debate sobre questões de privacidade no mundo virtual e o recolhimento de dados de usuários na Internet já se fazia presente no meio jurídico da União Europeia desde 1995 ao ser aprovada a diretiva 95/46 que unificou regras de proteção entre todos os países participantes da união. Ainda segundo LORENZON (2021), os desafios impostos pelo crescimento e avanço da internet fizeram com que União Europeia propusesse, em 2012, a *General Data Protection Regulation* (GDPR), que levaria quatro anos para ser elaborada e aprovada.

Para IRAMINA (2020), ao considerar que existem empresas operando em mais de um país, a convergência global das normas que regulam a proteção de dados tem-se mostrado fundamental para facilitar o fluxo de dados, o comércio e a cooperação entre organizações e autoridades públicas e também aumentando o nível de proteção de dados pessoais em todo mundo. A autora destaca também que grande parte das mais recentes legislações de proteção de dados são inspiradas no Regulamento Geral de Proteção de Dados (GDPR em inglês) da União Europeia.

Após a União Europeia divulgar o GDPR, o Senado Federal imediatamente validou o Projeto de Lei 53/18 atendendo como a Lei Geral de Proteção de Dados Brasileira (LGPD). (DA ROCHA *et al.*, 2019).

Conforme VIEIRA (2019), a LGPD regulamenta o uso, a proteção e a transferência de dados pessoais em território nacional, em âmbito público ou privado. O seu objetivo é garantir um efetivo controle por parte dos titulares sobre suas informações pessoais. O autor ainda expõe que, entre outras disposições, a LGPD exige consentimento explícito para coleta e uso dos dados e obriga a oferta de opções para o usuário visualizar, corrigir e excluir esses dados.

Segundo LORENZON (2021), a LGPD é um marco na legislação nacional por ter formulado diversos conceitos jurídicos novos como “dados pessoais”, “dados pessoais sensíveis”, “anonimização de dados”, entre outros para tratar do recolhimento, compartilhamento e uso de informações pessoais de indivíduos.

A LGPD, conforme o artigo 1º, se aplica a pessoas naturais ou por pessoas jurídicas de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade. (BRASIL 2018).

Segundo BRASIL (2018), o artigo 3º da Lei Geral de Proteção de Dados explica que a lei se aplica a qualquer operação de tratamento por pessoa natural ou jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou país onde estejam localizados os dados, desde que:

I. A operação de tratamento seja realizada no território nacional;
II. A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
III. Os dados pessoais objeto do tratamento tenha sido coletados no território nacional.

O artigo 4º dispõe que a lei não será aplicada nas seguintes hipóteses:

I. Realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
II. Realizados para fins exclusivamente:
    a. Jornalístico e artísticos;
    b. Acadêmicos;
III. Realizado para fins exclusivos de:
    a. Segurança pública;
    b. Defesa nacional;
    c. Segurança do Estado;
    d. Atividades de investigação e repressão penais.
IV. Provenientes de fora do território nacional que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

O artigo 5º formula diversos conceitos jurídicos novos, dos quais é possível destacar:

I. Dado pessoal: Informação relacionada a pessoa natural identificada ou identificável;

II. Dado pessoal sensível: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III. Dado anonimizado: Dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV. Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

V. Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VI. Anonimização: Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

VII. Tratamento: Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Segundo o artigo 6º da LGPD, o tratamento de dados pessoais deverá observar a boa-fé e os seguintes princípios: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Considerando os princípios acima, VIEIRA (2019) afirma que o princípio mais relevante é o da finalidade, por meio do qual os dados deverão ser utilizados apenas para finalidades específicas para as quais foram coletados e devidamente informadas aos titulares, juntamente com o princípio da minimização da coleta, ou seja, somente devem ser coletados os dados mínimos necessários para que seja atingida a finalidade, e o da retenção mínima, que determina a imediata exclusão dos dados após atingida a finalidade para a qual foram coletados.

O artigo 7º da LGPD dita as hipóteses de quando poderá ocorrer o tratamento de dados pessoais:

I. Mediante o fornecimento de consentimento pelo titular;
II. Para o cumprimento de obrigação legal ou regulatória pelo controlador;
III. Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas;
IV. Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V. Para a execução de contrato ou procedimentos preliminares que tenham relação com um contrato;
VI. Para o exercício regular de diretos em processo judicial, administrativo ou arbitral;
VII. Para a proteção da vida ou da incolumidade física do titular ou de terceiros;
VIII. Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
IX. Para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
X. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

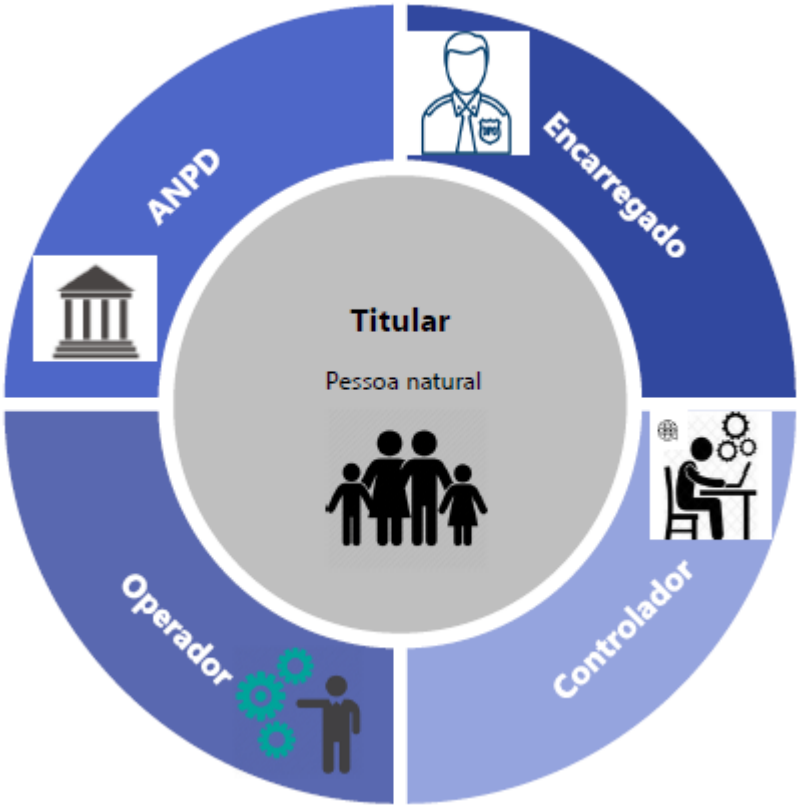
Ao que diz respeito aos direitos dos titulares sobre os seus dados pessoais, VIEIRA (2019), destaca o artigo 18 da LGPD, sobre o direito de o titular obter do controlador dos dados a qualquer momento a confirmação de existência de tratamento, a possibilidade de acesso, correção, anonimização, bloqueio, eliminação e portabilidade dos dados.

Conforme BRASIL (2020), é possível definir os atores envolvidos na lei, que são ilustrados na Figura 6:

- Titular: Qualquer pessoa natural, protegida pelo princípio da autodeterminação informativa;
- Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- Encarregado: Pessoa natural que faz a intermediação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

- Autoridade Nacional de Proteção de Dados (ANPD): tem a missão de regular o setor de tratamento de dados pessoais.

Figura 6 – Atores LGPD



Fonte: BRASIL (2020, p. 06).

Sobre a Autoridade Nacional de Proteção de Dados, VIEIRA (2019) explana que sua criação visa adequar a legislação brasileira no âmbito da proteção de dados, aos padrões internacionais. A ANPD é um órgão vinculado à Presidência da República, com autonomia técnica e a função de zelar, implementar e fiscalizar o cumprimento da LGPD.

No âmbito da Segurança e Sigilo de dados, a LGPD através do artigo 46 dispõe que 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.

O artigo 48 da LGPD explica que, em caso de incidente de segurança, o controlador deverá comunicar a autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. A comunicação deverá informar a

descrição dos dados pessoais afetados, informações sobre os titulares envolvidos, medidas de segurança utilizadas para a proteção dos dados, os riscos relacionados ao incidente e medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos de prejuízo.

No que diz respeito às Boas Práticas e Governança, a lei explica que os controladores e operadores poderão formular regras de boas práticas e de governança que contemplem os aspectos relacionados ao tratamento de dados pessoais.

Ainda referente às Boas Práticas e Governança, a LGPD no artigo 50 diz que o controlador poderá implementar um programa de privacidade que atenda no mínimo os requisitos:

a) Demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento de normas e boas práticas relativas à proteção de dados pessoais;
b) Seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) Seja adaptado à estrutura, escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
d) Estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
e) Tenha o objetivo de estabelecer relação de confiança com o titular;
f) Esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
g) Conte com planos de resposta a incidentes e remediação;
h) Seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

No que diz respeito à fiscalização, o artigo 52 dispõe sobre às sanções administrativas aplicáveis pela autoridade nacional:

I. Advertência, com indicação de prazo para medidas corretivas;
II. Multa simples, de até 2% do faturamento da pessoa jurídica no seu último exercício, limitada, no total à cinquenta milhões de reais por infração;
III. Multa diária;
IV. Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V. Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI. Eliminação dos dados pessoais a que se refere a infração;

VII. Suspenção parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de seis meses, prorrogável até a regularização da atividade de tratamento pelo controlador;

VIII. Suspenção do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período;

IX. Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados;

Nesse capítulo foi exposto o caminho que foi percorrido até o Brasil conseguir elaborar uma Lei de Proteção de Dados Pessoais. Foi exposta a aplicabilidade da Lei Geral de Proteção de Dados Brasileira, seus princípios, quando o tratamento de dados será realizado e o direito dos usuários em relação aos seus dados.

A LGPD trouxe importantes contribuições jurídicas ao definir termos e bases legais que deverão ser utilizadas para garantir a privacidade dos dados pessoais, bem como estabelecer sanções ao descumprimento da lei e exposição de dados.

É importante ressaltar que, por mais que a Lei tenha uma seção referente a Governança e Boas Práticas, ela não estabelece diretivas ou metodologias do que deve ser feito para que as empresas atinjam os objetivos expostos. Dessa forma, é importante que as empresas revejam seus processos e desenvolvam metodologias ou adotem estratégias que possam ser aproveitadas para o cumprimento da legislação. O próximo capítulo apresentará frameworks que podem ser utilizados como base para alcançar os objetivos da LGPD, bem como os objetivos estabelecidos para obtenção da certificação OEA.

5 FAMÍLIA DE PADRÕES - ISO 27000

Para RICARDO R. *et al.* (2015) a gestão da segurança da informação deve ser encarada, principalmente, como um processo de gestão (e não um processo tecnológico) que é obtido por meio da implantação de controles, políticas e procedimentos que, juntos, fortalecem os objetivos de negócio com a minimização dos seus riscos e a promoção da segurança da organização.

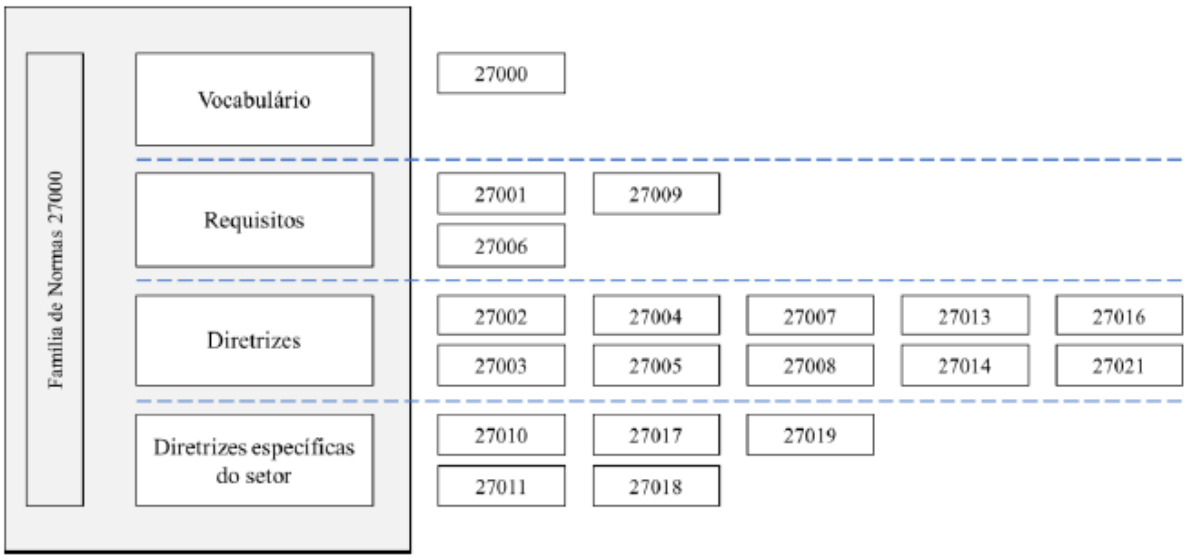
FERREIRA (2020) explica que a *International Organization for Standardization* (ISO) é uma entidade fundada em 1947, com sede na Suíça, responsável pelo desenvolvimento de *standards* a nível mundial nas mais diversas áreas. Em 1987, uniu-se com a *International Electrotechnical Comission* (IEC), entidade criada em 1906 na Suíça, e que desenvolve *standards* e sistemas de avaliação nas áreas de produtos, serviços e sistemas elétricos e eletrônicos. Ainda segundo FERREIRA (2020), esta comissão conjunta desenvolveu em 2005 a série de *standards* 27000 direcionada aos sistemas de gestão de segurança da informação.

Segundo a ISO/IEC 27000 (2018), a família de padrões de sistemas de gestão da segurança da informação consiste em padrões inter-relacionados, já publicados ou em desenvolvimento, e contém vários componentes estruturais significativos. Esses componentes estão focados em:

- Padrões que descrevem os requisitos do SGSI (ISO/IEC 27001);
- Requisitos do organismo de certificação (ISO/IEC 27006) para aqueles que certificam a conformidade com a ISO/IEC 27001;
- Estrutura de requisitos adicionais para implementações específicas do SGSI (ISO/IEC 27009)

Outros documentos fornecem orientação para vários aspectos da implementação de um SGSI, abordando um processo genérico, bem como orientação específica para o setor. (ISO/IEC 27000, 2018). A figura 7 ilustra a família de padrões do SGSI:

Figura 7 – Família de padrões do SGSI



Fonte: Ferreira (2020, p. 12).

Abaixo serão listados os padrões que são relevantes para o presente trabalho, sendo descritos por seu número de referência.

5.1 ISO/IEC 27000 - *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

A ISO/IEC 27000 é o documento que fornece uma visão geral da família de padrões relativas ao sistema de gestão de segurança da informação e a definição de todos os termos relacionados que são utilizados nas normas restantes. (FERREIRA, 2020)

A norma possui dentro do seu escopo fornecer para organizações e indivíduos:

a) Uma visão geral da família de padrões SGSI;
b) Uma introdução aos sistemas de gestão de segurança da informação
c) Termos e definições usados em toda a família de padrões SGSI.

5.2 ISO/IEC 27001 - *Information technology — Security techniques — Information security management systems — Requirements*

A ISO/IEC 27000 (2018) define como escopo da ISO/IEC 270001 especificar os requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar os sistemas de gestão de segurança da informação (SGSI). A norma fornece requisitos normativos para o desenvolvimento e operação de um SGSI, incluindo um conjunto de

controles para vigilância e mitigação dos riscos associados aos ativos de informação que a organização busca proteger operando seu SGSI.

Para MAGALHÃES (2021), o foco principal da ISO 27001 é proteger a integridade, confidencialidade e disponibilidade das informações em uma empresa. Para o autor, isso é feito descobrindo quais são os potenciais problemas que podem acontecer com as informações (avaliação de risco) e, em seguida, definindo o que precisa ser feito para evitar que tais problemas aconteçam (mitigação de risco).

FERREIRA (2020) destaca que a norma concede bastante importância aos processos de avalição e tratamento dos riscos e baseia a sua dinâmica e implementação no ciclo PDCA (*plan-do-check-act*). Este ciclo é um método iterativo de controle e de melhoria contínua, seu objetivo é que as organizações melhorem os seus processos de forma contínua e consigam, assim, identificar e corrigir falhas e aperfeiçoar a sua performance. A figura abaixo ilustra o ciclo PDCA e seus processos:

Figura 8 – Ciclo PDCA

Fonte: Adaptado de Ferreira (2020, p. 14).

Referente ao contexto da organização, a norma define que a organização deve determinar as questões internas e externas que são relevantes para o seu propósito e que afetam a sua capacidade para alcançar os resultados pretendidos do seu sistema de gestão de segurança da informação.

Ao abordar a liderança, a NBR ISO/IEC 27001 explica que a alta direção deve demonstrar a sua liderança e comprometimento em relação ao sistema de gestão da segurança

da informação, assegurando que a política e objetivos de segurança da informação sejam compatíveis com a direção estratégica da organização, garantindo a integração dos requisitos do SGSI dentro dos processos da organização, assegurando a disponibilidade dos recursos necessários para o SGSI, comunicando a importância de uma gestão eficaz da segurança da informação, assegurando que o SGSI alcança seus resultados pretendidos, promovendo melhoria continua e apoiando outros papéis relevantes da gestão para demonstrar como sua liderança se aplica às áreas sob sua responsabilidade.

Quanto ao planejamento, a organização deve considerar o contexto da organização e as necessidades e expectativas e determinar os riscos e oportunidades para que o SGSI alcance os resultados pretendidos, previna ou reduza os efeitos indesejados e alcance a melhoria contínua.

A norma ainda detalha que a organização deve estabelecer os objetivos de segurança da informação para as funções e níveis relevantes. Os objetivos da segurança da informação devem ser consistentes com a política de segurança da informação, serem mensuráveis (quando possível), levar em conta os requisitos de segurança da informação aplicáveis e os resultados da avaliação e tratamento de riscos, os objetivos devem ser comunicados e devem ser atualizados conforme o apropriado.

Ainda ao tratar do planejamento, é abordado no padrão que a organização deve reter informação documentada dos objetivos de segurança da informação. No que diz respeito ao planejamento para alcançar os objetivos, a organização deve determinar:

- O que será feito;
- Quais recursos serão necessários;
- Quem será responsável;
- Quando estará concluído;
- Como os resultados serão avaliados.

Na etapa de apoio, a NBR ISO/IEC 27001 dita que a organização deve determinar e prover recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do SGSI. Além disso, a organização deve determinar a competência necessária das pessoas que realizam o trabalho e que afetam o desempenho da segurança da informação, também deve assegurar que essas pessoas são competentes, com base na educação, treinamento ou experiência apropriados.

Ao se referir sobre as pessoas que realizam o trabalho sob controle da organização, a norma rege que as pessoas devem estar cientes da política de segurança da informação, suas

contribuições para a eficácia do SGSI e as implicações da não conformidade com os requisitos do sistema.

A organização deve determinar as comunicações internas e externas para o sistema de gestão da segurança da informação incluindo o que comunicar, para quem, quando e quem será comunicado.

Na operação, a norma rege que a organização deve planejar, implementar e controlar os processos necessários para atender os requisitos de segurança da informação. Deve realizar avaliações dos riscos de segurança da informação a intervalos planejados, ou quando mudanças significativas são propostas ou ocorrem, também rege que a organização deve implementar o plano de tratamento de riscos de segurança da informação.

Para realizar a avaliação de desempenho a ISO/IEC 27001 cita que é necessário avaliar o desempenho da segurança da informação e eficácia do SGSI. A organização deve determinar o que precisa ser monitorado e medido, incluindo controles e processos de segurança da informação. Também deve determinar os métodos de monitoramento, medição, análise e avaliação, quando o monitoramento e medição devem ser realizados, o que deverá ser monitorado e medido, quando os resultados serão analisados e avaliados e quem deve analisar estes resultados.

A auditoria interna da organização deve prover informações sobre o quanto o SGSI está em conformidade com os requisitos da organização e os requisitos da norma NBR ISO/IEC 27001.

A alta direção deve analisar criticamente o sistema de gestão da segurança da informação em intervalos planejados, para assegurar a sua contínua adequação, pertinência e eficácia.

No processo de melhoria, a norma cita que quando uma não conformidade ocorre, a organização deve reagir a não conformidade e, conforme avaliação, tomar ações para controlar e corrigi-la e tratar as consequências, além de avaliar a necessidade de ações para eliminar as causas da não conformidade.

A norma frisa que a organização deve continuamente melhorar a pertinência e eficácia do sistema de gestão da segurança da informação.

5.3 ISO/IEC 27002 - *Information technology — Security techniques — Code of practice for information security controls*

FERREIRA (2020) afirma que a ISO/IEC 27002 fornece diretrizes para a

implementação dos controles de segurança cedidos na norma ISO/IEC 27001. ALENCAR, DE MOURA e JUNIOR (2017) explicam que a norma pode ser entendida como um código completo de controles que auxiliam a aplicação do SGSI. Ainda, segundo ALENCAR; DE MOURA; JUNIOR (2017), apesar de ser recomendável sua utilização em conjunto com a ISO 27001, a norma pode ser consultada de forma independente com fins de adoção de boas práticas.

MAGALHÃES (2021) discorre que a ISO/IEC 27002 é um código de prática, um documento para consulta genérico e não é uma especificação formal como a ISO 27001. Para MAGALHÃES (2021), a norma recomenda que exista controle relativamente à segurança da informação e que seja abordado os objetivos sobre o controle de segurança da informação decorrentes de riscos à confidencialidade, integridade e disponibilidade da informação. A norma contém 14 seções de controles da segurança da informação.

A seção 5 da norma trata sobre as políticas de segurança da informação. A seção dispõe que um conjunto de políticas da segurança da informação seja definido, aprovado pela direção, publicado e comunicado para funcionários e partes externas relevantes.

Organização da segurança da informação é o tema abordado na seção 6 da NBR ISO/IEC 27002, cujo objetivo é estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação da segurança da informação dentro da organização. Todas as responsabilidades pela segurança da informação devem ser definidas e atribuídas e feitas em conformidade com as políticas de segurança da informação. As responsabilidades pela proteção de cada ativo e pelo cumprimento dos processos de segurança da informação devem ser claramente definidas, assim como as responsabilidades pelas atividades do gerenciamento dos riscos de segurança da informação e, em particular, pela aceitação dos riscos residuais.

A seção 7 trata sobre a segurança em Recursos Humanos. A norma é dividida em momentos. Antes da contratação o objetivo da seção é assegurar que funcionários e partes externas entendam as suas responsabilidades e estão em conformidade com os papéis para o que foram selecionados. Durante a contratação o objetivo é assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação. No encerramento e mudança da contratação o objetivo é proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.

A norma também trata sobre a responsabilidade pelos ativos em sua oitava seção, tendo por objetivo identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos.

O controle de acesso é abordado na seção 9, definindo como objetivo limitar o acesso à informação e aos recursos de processamento da informação. Isso é feito com a implementação de uma política de controle de acesso, baseada nos requisitos da segurança da informação e negócios. É estabelecido também a implementação das diretivas de acesso às redes e aos serviços de redes, que convém que os usuários recebam acesso as redes e aos serviços de rede que tenham sido especificamente autorizados a usar. A seção 9 registra também as diretivas para gerenciamento de acesso ao usuário que tem como objetivo assegurar o acesso de usuário autorizado e prevenir o acesso não autorizado a sistemas e serviços. Estabelece também as responsabilidades dos usuários e controle de acesso ao sistema, cujo objetivos são tornar os usuários responsável pela proteção das suas informações de autenticação e prevenir o acesso não autorizado a sistemas, respectivamente.

A seção 10 diz respeito à Criptografia e visa assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e integridade da informação. Estabelece que devam ser desenvolvidas e implementadas políticas para o uso de controles criptográficos, assim como estabelece o controle de Gerenciamento de Chaves, uma política sobre o uso, proteção e tempo de vida das chaves criptográficas.

A seção 11 é responsável por tratar a Segurança Física e do ambiente, seu objetivo é estabelecer áreas seguras, prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e nas informações da organização.

A Segurança nas Operações é tratada na seção 12, com objetivo de garantir a operação segura e correta dos recursos de processamento da informação. Estabelece a gestão de mudanças para que as mudanças na organização, processos e recursos de processamento da informação que afetam a segurança da informação sejam controladas. Gestão de capacidade que é a utilização dos recursos monitoradas para garantir o desempenho dos sistemas. Separação dos ambientes de desenvolvimento, teste e produção, para promover a redução dos riscos de acessos ou modificações não autorizadas no ambiente de produção.

Ainda no tema da Segurança das Operações, é abordado a proteção contra *malware,* cujo objetivo é assegurar que as informações e recursos estão protegidos contra *malware.* Estabelece que sejam implementados controles de detecção, prevenção e recuperação para proteger contra as ameaças, combinados com um programa de conscientização do usuário. Outro tópico importante dentro da Segurança nas Operações é o estabelecimento de cópias de segurança para proteção contra a perda de dados, definindo que essas cópias sejam efetuadas e testadas regularmente.

A NBR ISO/IEC 27002 através da seção 13 trata a Segurança nas comunicações, um dos tópicos é o Gerenciamento da Segurança em Redes, que estabelece controles visando assegurar a proteção das informações em redes e dos recursos de processamento da informação que as apoiam. Trata ainda a Transferência de Informação com controles que propõem manter a segurança da informação transferida dentro da organização e com quais quer entidades externas.

A seção 14 da norma trata e explica as políticas para a Aquisição, desenvolvimento e manutenção de sistemas. Seu objetivo é garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação.

O Relacionamento na Cadeia de Suprimento é abordada na seção 15 e engloba a segurança da informação na cadeia de suprimento, estabelecendo diretrizes para garantir a proteção dos ativos da organização que são acessados pelos fornecedores, que pode ser realizado através de política de segurança da segurança da informação no relacionamento com os fornecedores. É estabelecido também um controle de Gerenciamento de Entrega do Serviço do Fornecedor, cujo objetivo é manter um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.

Através da seção 16, o tema abordado é a Gestão de Incidentes de Segurança da Informação. Como objetivo, busca assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação. São estabelecidos responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação. Também é elaborado o controle de notificação de eventos de segurança da informação, onde os eventos de segurança da informação sejam relatados por meio dos canais de gestão o mais rápido possível.

Outro controle importante da seção é a notificação de fragilidades de segurança da informação, onde é instruído que os funcionários e partes externas que utilizam os sistemas de informação sejam instruídos a registrar e notificar quaisquer fragilidades de segurança da informação. Os incidentes de segurança da informação devem ser avaliados, possuir uma resposta, deve ser realizada a coleta de evidências e, se possível, obter conhecimento do incidente.

Na penúltima seção da norma, os Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio são abordados. É apontada a continuidade da segurança da informação, ditando que a continuidade da segurança da informação seja contemplada nos

sistemas de gestão da continuidade do negócio da organização. É indicado que os recursos de processamento da informação possuam redundância para assegurar a sua disponibilidade.

A 18ª e última seção da norma ISO/IEC 27002 dispõe sobre a Conformidade, visando evitar a violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança. Trata a análise crítica da segurança da informação, cujo objetivo é garantir que a segurança da informação esteja implementada e operada de acordo com as políticas e procedimentos da organização.

5.4 ISO/IEC 27701 - *Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

A ISO/IEC 27701 (2019) fornece as diretrizes para implementação, manutenção e melhoria contínua de um sistema de gestão de privacidade, sendo uma extensão das normas ISO/IEC 27001 e ISO/IEC 27002 para a gestão da privacidade dentro das organizações.

A seção 5 da norma apresenta os requisitos específicos para um sistema de gestão da privacidade (SGPI) e outras informações relacionadas à segurança da informação da ISO/IEC 27001.

As diretrizes de um SGPI e outras informações relacionadas aos controles de segurança da informação contidos na ISO/IEC 27002 são apresentadas na seção 6 da norma.

Na seção 7 e 8 da ISO/IEC 27701 são expostas as diretrizes adicionais da norma 27002 para os controladores e operadores de dados pessoais, respectivamente.

6 COBIT 5

O COBIT foi desenvolvido pela *Information Systems Audit and Control Association* (ISACA) e tem sido internacionalmente aceito como boa prática para controle de TI, estabelecendo um modelo de domínios e processos com a apresentação de atividades em uma estrutura lógica e gerenciável, com foco no controle e não na execução. (SANTOS, 2013).

RIOS; TEIXEIRA FILHO; DA SILVA RIOS (2017) explicam que o COBIT 5 fornece um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI, mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e o uso de recursos. Citando Gehrmann (2012), RIOS; TEIXEIRA FILHO; DA SILVA RIOS (2017) observam que o COBIT não define como os processos serão executados, mas possibilita controles básicos para que a tecnologia da informação alcance seus objetivos alinhados aos objetivos de negócio da organização.

PEREIRA e FERREIRA (2015) destacam que o COBIT 5 fornece um *Framework* compreensivo que auxilia as organizações a alcançar os seus objetivos para a governança e gestão da TI, de uma forma holística a toda organização, isto é, englobando as diversas áreas de negócio e a TI.

Segundo ISACA (2012), o COBIT 5 baseia-se em cinco princípios básicos para a governança e gestão de TI da organização, que são ilustrados na figura abaixo:

Figura 9 – Princípios do COBIT 5

Fonte: ISACA (2012, p. 15).

1º Princípio - Atender às necessidades das partes interessadas: ISACA (2012) afirma que organizações existem para criar valor para suas partes interessadas mantendo o equilíbrio entre a realização de benefícios e a otimização do risco e uso dos recursos. O COBIT 5 visa fornecer os processos necessários para a criação de valor para a organização com o uso de TI.

2º Princípio – Cobrir a organização de ponta a ponta: O COBIT 5 aborda a governança e gestão da informação e da tecnologia a partir da perspectiva de toda a organização, isso implica que o COBIT:

- Integra a governança corporativa de TI à governança corporativa da organização, ou seja, o sistema de governança corporativa de TI integra-se em qualquer sistema de governança.
- Cobre todas as funções e processos necessários para regular e controlar as informações da organização e tecnologias correlatas. O COBIT 5 trata de todos os serviços internos e externos pertinentes, bem como dos processos de negócios internos

3º Princípio – Aplicar um *Framework* Único e Integrado: O COBIT 5 alinha-se com outros padrões e modelos, permitindo que a organização utilize o COBIT 5 como principal integrador do modelo de governança e gestão.

4º Princípio – Permitir uma Abordagem Holística: Introduz os habilitadores, fatores que influenciam se algo irá funcionar. O modelo do COBIT 5 descreve sete categorias de habilitadores que estão ilustradas na Figura 10:

- Princípios, Políticas e frameworks: São veículos para a tradução do comportamento desejado em orientações práticas para a gestão diária;
- Processos: descrevem um conjunto de práticas e atividades para atingimento de determinados objetivos e produzem um conjunto de resultados em apoio aos objetivos de TI.
- Estrutura organizacionais: São as principais entidades de tomada de decisão em uma organização.
- Cultura, ética e comportamento: Das pessoas e organização são muitas vezes subestimados como fator de sucesso nas atividades de governança e gestão.
- Informação: Inclui todas as informações produzidas e usadas pela organização. É necessária para manter a organização em funcionamento e bem governada.

- Serviços, infraestrutura e aplicativos: Fornecem à organização o processamento e os serviços de tecnologia da informação.
- Pessoas, habilidades e competências: Estão associadas às pessoas e são necessárias para a conclusão bem-sucedida das atividades e para a tomada de decisões assertivas e tomada de medidas corretivas.

Figura 10 – Habilitadores Corporativos do COBIT 5

Fonte: ISACA (2012, p.29)

5º Princípio – Distinguir Governança e Gestão: Faz distinção entre governança e gestão. Segundo a norma, a distinção entre governança e gestão é:

- Governança: Garante que as necessidades, condições e opções das partes interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados; definindo a direção através de priorizações e tomadas de decisão e monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos.
- Gestão: É responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades em consonância com a direção definida pelo órgão de governança a fim de atingir os objetivos corporativos.

6.1 MODELO DE CAPACIDADE DE PROCESSO DO COBIT 5

Os modelos de maturidade de processo são usados para medir a maturidade atual ou “o estado em que se encontra” dos processos de TI de uma organização para definir o estado de

maturidade necessário e para determinar a diferença entre eles e como melhorar o processo para atingir o nível de maturidade desejado. (ISACA, 2012).

Ainda segundo a ISACA (2012), o COBIT 5 possui um modelo de capacidade de processo com base na ISO/IEC 15504. Esse modelo proporciona meios para medir o desempenho de processos de governança ou processos de gestão e permite a identificação das áreas que precisam ser melhoradas.

Quadro 5 – Níveis de Capacidade e Atributos de Processo

ID de Atributo de Processo	Níveis de Capacidade e Atributos de Processo
	Nível 0: Processo Incompleto
	Nível 1: Processo Executado
P.A 1.1	Execução do Processo
	Nível 2: Processo Gerenciado
P.A 2.1	Gestão da Execução
P.A 2.2	Gestão dos Produtos de Trabalho
	Nível 3: Processo Estabelecido
P.A 3.1	Definição do Processo
P.A 3.2	Implementação do Processo
	Nível 4: Processo Previsível
P.A 4.1	Gestão do Processo
P.A 4.2	Controle do Processo
	Nível 5: Processo Otimizado
P.A 5.1	Inovação do Processo
P.A 5.2	Otimização do Processo

Fonte: Adaptado de ISACA (2012, p. 13).

Conforme Listado no Quadro 5, o COBIT 5 define que um processo pode atingir seis níveis de capacidade, incluindo uma designação de "processo incompleto" caso suas práticas não atinjam o objetivo do processo:

0. Processo Incompleto – O processo não foi implementado ou não atingiu seu objetivo. Neste nível, há pouca ou nenhuma evidência de qualquer atingimento sistemático do objetivo do processo.
1. Processo Executado – O Processo Implementado atinge seu objetivo.

1.1. Execução do Processo – Existe evidência de que o processo atinge seu objetivo.

2. Processo Gerenciado – O processo realizado agora é implementado de forma administrativa (planejado, monitorado e ajustado) e seus produtos do trabalho são adequadamente estabelecidos, controlados e mantidos.
   2.1. Gestão da execução – Atributo onde o desempenho do processo é gerenciado.
   2.2. Gestão dos Produtos de trabalho – Atributo em que os produtos do trabalho produzidos pelo processo são gerenciados de forma apropriada. Os produtos de trabalho são aqueles que resultam da obtenção dos resultados do processo.
3. Processo Estabelecido – O Processo controlado descrito agora é implementado utilizando um processo definido capaz de atingir seus resultados.
   3.1. Definição do Processo – Atributo em que um processo padrão é mantido para apoiar a implantação do processo definido.
   3.2. Implementação do Processo – Atributo em que o processo padrão é efetivamente implantado como um processo definido para atingir os resultados do processo.
4. Processo Previsível – O processo criado opera agora dentro dos limites definidos para produzir seus resultados.
   4.1. Gestão do Processo – Atributo em que os resultados da medição são usados para garantir que o desempenho do processo apoie a realização dos objetivos de desempenho do processo relevantes em apoio às metas de negócios definidas.
   4.2. Controle do Processo – Atributo onde o processo é gerenciado quantitativamente para produzir um processo que é estável, capaz e previsível dentro de limites definidos.
5. Processo Otimizado – O processo é continuamente melhorado visando o atingimento dos objetivos corporativos pertinentes, atuais ou previstos.
   5.1. Inovação do Processo – Atributo em que as mudanças no processo são identificadas a partir da análise das causas comuns de variação no desempenho e das investigações de abordagens inovadoras para a definição e implantação do processo.
   5.2. Otimização do processo – Atributo onde as mudanças na definição, gestão e desempenho dos processos resultam em impacto efetivo que atinge os objetivos de melhoria de processos relevantes.

Segundo ISACA (2012), cada nível de capacidade só pode ser atingido quando o nível anterior tiver sido plenamente alcançado. Explica também, que há uma diferença significativa entre a capacidade de processo nível 1 e os níveis mais altos. Atingir a capacidade de processo nível 1 exige que o atributo de desempenho do processo seja amplamente atingido, o que, de fato, significa que o processo está sendo realizado com sucesso e os resultados esperados

estão sendo obtidos pela organização. Níveis de capacidade mais altos adicionam então diferentes atributos a ele. Neste esquema de avaliação, atingir a capacidade nível 1, mesmo em uma escala de 5, já pode ser considerada uma importante conquista para a organização.

Cada atributo é classificado usando uma escala de classificação padrão definida na ISO/IEC 15504. Sendo estas:

- **N – Não Alcançado.** Há pouca ou nenhuma evidência de alcance do atributo definido no processo avaliado.
- **P – Parcialmente Alcançado.** Há algumas evidências de uma abordagem e alguma realização do atributo definido no processo avaliado. Alguns aspectos da obtenção do atributo podem ser imprevisíveis.
- **L – Amplamente Atingido.** Há evidência da abordagem sistemática e atingimento significativo do atributo definido no processo avaliado. Alguns pontos fracos referentes a este atributo podem existir no processo avaliado.
- **F – Plenamente atingido.** Há evidência da abordagem completa e sistemática e pleno atingimento do atributo definido no processo avaliado. Não existe nenhum ponto fraco significativo referente a este atributo no processo avaliado.

É necessário garantir um grau consistente de interpretação ao decidir qual classificação atribuir (ISACA, 2012). A tabela abaixo descreve a classificação em termos de porcentagem alcançada:

Quadro 6 – Níveis de Classificação

Abreviação	Descrição	% Alcançada
N	Não Alcançado	0 a 15% alcançado
P	Parcialmente Alcançado	15% a 50% alcançado
L	Amplamente Atingido	50% a 85% alcançado
F	Plenamente Atingido	85% a 100% alcançado

Fonte: adaptado de ISACA (2012, p. 14).

O modelo de capacidade de processo do COBIT 5 apresenta uma alternativa viável para o desenvolvimento de um modelo de maturidade de processos para um *framework* de segurança da informação, visando a certificação OEA e a adequação a LGPD.

7 REVISÃO DA LITERATURA

Para o desenvolvimento da presente publicação foi realizada revisão da literatura em busca de modelos, sistemas, *frameworks* de segurança da informação que suportem o desenvolvimento de um *framework* da segurança da informação com aderência à OEA e que cumpra os requisitos exigidos pela LGPD.

Para realizar a pesquisa, foram utilizados diversos sites de pesquisa acadêmica, tendo se destacado pela relevância dos resultados os sites Google Acadêmico e EBSCOhost. Foram utilizadas palavras-chave para a realização das pesquisas, tais como “OEA”, “LGPD”, “Segurança da Informação”, “ISO 27000”, “Comércio exterior”.

Para a pesquisa da Legislação, a principal fonte de informação foram os sites do Governo Federal Brasileiro – Portal GOV.BR. Também foram utilizados os sites de pesquisa Google e Bing para pesquisas complementares de legislação.

Durante a revisão da literatura foi observada a falta de trabalhos acadêmicos voltados à segurança da informação no âmbito do programa brasileiro de Operador Econômico Autorizado, ressaltando a importância no desenvolvimento do trabalho atual. Entre os trabalhos pesquisados, as obras de DA ROCHA *et al.* (2019) e PARANHOS (2010) se destacam como modelos a serem estudados e que podem servir de base para o desenvolvimento do framework proposto.

DA ROCHA *et al.* (2019) analisam como a ISO 27001 pode ser usada como ferramenta de controle para a LGPD. O estudo analisa como um SGSI irá ajudar no controle das regras fazendo com que a organizações possam atingir qualidades necessárias para se adequar a segurança dos dados no âmbito da LGPD.

Entre os objetivos do trabalho DA ROCHA *et al.* (2019), elencam identificar as principais características da LGPD, citar os pontos mais relevantes da ISO 27001, comparar a norma ISO 27001 com a LGPD e apresentar uma tabela identificando os pontos de conformidade entre a lei e a normativa ISO.

Entre os pontos mais relevantes da Lei, os autores elencam como desafios para as empresas:

- Nomeação de um encarregado – DPO;
- Realização de auditoria de dados;
- Elaboração de mapa de dados;
- Mudanças nas políticas de segurança;
- Revisão de contratos;

- Criação de Relatório de Impacto de Privacidade.

Através de pesquisa bibliográfica os autores comparam a Lei à norma, identificando os pontos de associação entre ambas, foi elaborada uma tabela de comparação entre a Lei Geral de Proteção dos Dados e a norma ISO 27001 com 12 pontos que mostram como é possível ajudar as empresas a entrarem em conformidade com a LGPD.

Segundo o estudo realizado pelos autores, 42% dos artigos da LGPD estão cobertos pela ISO 27001, 48% dos artigos estão relacionados diretamente ou indiretamente com a normativa e 10% dos artigos não estão cobertos.

Foi concluído pelos autores que a pesquisa possibilitou uma análise de como a ISO 27001 pode auxiliar as empresas a entrarem em conformidade com a LGPD, ressaltando que empresas que já possuem certificação possivelmente já adotaram as medidas para o cumprimento da legislação brasileira de dados. É apontado também a necessidade de trabalhos futuros que solucionem os 10% da LGPD que não foram supridos pela lei que está relacionada a ANPD.

Um dos objetivos específicos expostos no presente trabalho é elaborar níveis de maturidade para o framework desenvolvido. PARANHOS (2010) propôs um framework de segurança da informação para identificação do nível de maturidade das organizações, identificação do nível de maturidade exigido pelo negócio e a identificação dos controles necessários para atender esses níveis com a priorização correta. O autor analisou diversos documentos e assuntos referentes à segurança e informação e os dividiu em 10 domínios principais.

Assim, o framework possibilitou a comparação entre o nível de maturidade exigido pelo negócio e o nível de maturidade atual, identificando as lacunas existentes e possibilitando a priorização de investimentos em segurança da informação dadas as necessidades do negócio.

Como conclusão, o autor destaca que o framework conseguiu atingir o objetivo de ser um ponto de apoio para a gestão da segurança da informação nas corporações, identificando os níveis de maturidades da organização e o nível exigido pelo negócio. Como possibilidade de trabalho futuro, é destacada a aplicação do framework em um número maior de empresas para validar a sua real aplicabilidade e necessidade.

8 OAS FRAMEWORK

O OAS Framework – Operador Autorizado Seguro Framework – foi desenvolvido para suprir as necessidades das empresas que buscam se adequar aos critérios de elegibilidade da gestão da informação que compreendem aos requisitos de segurança da informação para obter a certificação OEA e que buscam estar de acordo com a LGPD.

O OAS está apoiado nos itens dispostos nas normas da família ISO 27000 e está dividido em 6 módulos que contém as diretrizes para a adequação aos requisitos propostos pela legislação de proteção de dados pessoais e pela RFB no que tange a certificação OEA.

8.1 OAS – Política de Segurança da Informação

A alta direção deve estabelecer uma política de segurança da informação que seja apropriada ao propósito da organização e que busque a conformidade com os itens dispostos na certificação de Operador Econômico Autorizado. Segundo o item 5.2 da ISO 27001 a política deve incluir os objetivos da segurança da informação ou fornecer a estrutura para estabelecer os objetivos de segurança da informação. Também deve ser incluído na política o comprometimento em satisfazer os requisitos aplicáveis relacionados com a segurança da informação e o comprometimento com a melhoria contínua do sistema de gestão da segurança da informação.

A política da segurança da informação deve estar disponível como informação documentada, ser comunicada dentro da organização e estar disponível para as partes interessadas.

A ISO 27002 demonstra que um conjunto de políticas de segurança da informação deve ser definido pela alta direção, aprovado, publicado e comunicado para todos funcionários e partes externas relevantes. Para sua implementação, a política deve contemplar requisitos oriundos de:

a) Estratégia do negócio;
b) Regulamentações, legislação e contratos;
c) Ambiente de ameaça da segurança da informação;

A política de segurança da informação deve conter declarações relativas à definição de segurança da informação, seus objetivos e princípios, para que sejam orientadas as atividades relativas à segurança da informação. Devem ser dispostas as atribuições de responsabilidades,

gerais e específicas, para o gerenciamento da segurança da informação para cada papel. E que seja explícito os processos para o tratamento dos desvios e exceções.

Em nível mais baixo, a política de segurança da informação deve ser apoiada por políticas específicas do tema, que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades da organização. O item 5.1.1 da ISO 27002 fornece exemplos de tais temas de política: Controle de acesso, segurança física e do ambiente, uso dos ativos, mesa limpa e tela limpa, transferência de informações, dispositivos móveis e trabalho remoto, restrições de uso e instalação de *software, backup,* transferência de informação, proteção contra *malware,* gerenciamento de vulnerabilidades técnicas, controles criptográficos, segurança nas comunicações, proteção e privacidade da informação de identificação pessoal e relacionamento na cadeira de suprimento. Em especial, durante o desenvolvimento e manutenção de políticas de segurança de informação, a organização deve considerar a legislação de proteção de dados pessoais a fim de estar atendendo a legislação.

Ao implementar uma Política de Segurança da Informação, a organização além de estar comprometida com a continuidade do negócio, segurança dos seus sistemas e proteção de dados pessoais, está cumprindo com os requisitos dispostos na OEA e LGPD, no que abrangem as boas práticas de governança.

8.2 OAS – Política de Backup

Conforme o critério da OEA, as informações relacionadas com as operações de comércio exterior devem ser armazenadas de forma que possibilite sua restauração. As cópias de segurança das informações devem ser efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida. A política de *backup* deve ser estabelecida para definir os requisitos da organização relativos às cópias de segurança das informações*, softwares* e sistemas.

Segundo a ISO 27002, na elaboração de um plano de *backup*, os seguintes itens devem ser levados em consideração:

a) Registros completos e exatos das cópias de segurança e documentação apropriada sobre os procedimentos de restauração da informação;
b) A abrangência e frequência da geração das cópias reflitam os requisitos de negócio, além dos requisitos da segurança da informação, bem como a sua criticidade para a continuidade da operação.;

c) As cópias devem ser armazenadas em localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no próprio local principal;
d) As mídias de *backup* devem ser regularmente testadas para garantir que sejam confiáveis no caso do uso emergencial. Isto deve ser combinado com um teste de restauração e checado contra o tempo de restauração requerido.;
e) Em situações em que a confidencialidade é importante, as cópias de segurança devem ser protegidas através de encriptação;
f) Ao restaurar dados pessoais, deve ser gerado registro da restauração do dado pessoal contendo o nome da pessoa responsável pela restauração e a descrição do dado pessoal restaurado.

Devem ocorrer procedimentos operacionais para monitorar a execução dos *backup*s e apontem falhas de *backup* programado, para garantir a integralidade das cópias. Tais cópias devem ser testadas regularmente para garantir que estão aderentes aos requisitos definidos nos planos de continuidade do negócio.

8.3 OAS – Política de Privacidade

A organização deve produzir uma Política de Privacidade que demonstre o seu comprometimento para obter aderência com as legislações de dados pessoais, e com termos contratuais acordados entre a organização e seus parceiros e terceiros aplicáveis, explicitando as responsabilidades na relação comercial.

A LGPD dispõe sobre o tratamento de dados pessoais com o objetivo de proteger os direitos de liberdade e privacidade, assim, qualquer operação de tratamento de dados realizado por pessoa natural ou jurídica é regida por esta lei.

A Política de Privacidade deve explicar quais dados são utilizados pelo controlador, quais dados podem ser coletados automaticamente durante a utilização das páginas de rede (Exemplo: IP, características do navegador, data e hora do acesso) ou dados fornecidos pelo próprio titular. Deve informar quais tecnologias são empregadas para tal coleta, tais como *cookies* e *beacons*.

A finalidade para o tratamento dos dados pessoais deve ser abordada pela política desenvolvida. A organização deve assegurar que os titulares de dados pessoais entendam o propósito pelos quais seus dados serão tratados. Sem uma clara declaração do propósito para tratamento, não é possível que o consentimento e as escolhas sejam dados adequadamente.

Em caso de compartilhamento de dados com terceiros, a organização deve informar com quem o dado pessoal foi compartilhado e a finalidade para o compartilhamento.

Em cumprimento à legislação Brasileira no que tange o tratamento de dados pessoais, a organização deve informar os direitos do usuário perante seus dados. Bem como deve informar os meios disponíveis para entrar em contato com o Encarregado pelo Tratamento de Dados Pessoais para tratar sanar dúvidas pertinentes sobre a política de privacidade, atendimento de solicitações relacionadas aos seus dados ou apresentar queixa referente à possível violação da LGPD.

As especificações para cumprimento dos itens relacionados ao tratamento de dados pessoais acima constam no módulo 6 do OAS Framework e podem estar explicitados na política de privacidade para melhor entendimento do titular dos dados pessoais.

8.4 OAS – Restrição à informação

Um dos critérios de elegibilidade relacionado à segurança da informação da OEA dispõe que todas as informações relacionadas com as operações de comércio e exterior e dados pessoais devem estar protegidas contra acesso não autorizado e situações acidentais ou ilícitas de destruição, perda, alteração ou qualquer forma de tratamento ilícito.

As restrições para o acesso devem ser baseadas nos requisitos das aplicações do negócio e de acordo com a política de controle de acesso definida. Os seguintes controles foram implementados pelo item 9.4.1 da ISO 27702 e devem ser considerados de forma a apoiar os requisitos de restrição de acesso:

a) Fornecer menus para controlar o acesso às funções dos sistemas de aplicação;
b) Controlar quais dados podem ser acessados por um usuário em particular;
c) Controlar os direitos de acesso dos usuários, por exemplo, ler, excluir e executar;
d) Controlar os direitos de acesso de outras aplicações;
e) Limitar a informação contida nas saídas;
f) Prover controles de acesso lógico ou físico para o isolamento de aplicações sensíveis, dados de aplicação ou sistemas.

8.4.1 OAS – Controle de Acesso às Informações

Uma política de controle de acesso deve ser estabelecida, documentada e analisada baseada nos requisitos de segurança da informação e dos negócios. O item 9 da ISO 27002 explica que a política de controle de acesso deve levar em consideração os seguintes itens:

a) Requisitos de segurança de aplicações de negócios individuais;
b) Política para disseminação e autorização da informação, por exemplo a necessidade de conhecer, onde o usuário somente tem permissão para acessar informação que necessita para desempenhar suas tarefas;
c) Legislação pertinente e qualquer obrigação contratual relativa à proteção de acesso para dados ou serviços;
d) Segregação de funções de controle de acesso, por exemplo, pedido de acesso, autorização de acesso, administração de acesso;
e) Requisitos para autorização formal de pedidos de acesso;
f) Remoção de direitos de acesso;
g) Arquivo dos registros de todos os eventos significantes, relativos ao uso e gerenciamento das identidades do usuário e de senhas;

Os usuários somente devem ter acesso às redes e serviços de rede que tenham sido especificamente autorizados a usar. Uma política com relação ao uso de redes e serviços de rede pode ser elaborada, esta política deve ser consistente com a política de controle de acesso e deve incluir:

a) Redes e serviços de redes que são permitidos de serem acessados;
b) Procedimentos de autorização para determinar quem tem permissão para acessar quais redes e serviços de redes;
c) Controles de gerenciamento para proteger o acesso a conexões e serviços de rede;
d) Os meios usados para acessar redes e serviços de rede (exemplo, uso de VPN ou redes sem fio);
e) Monitoramento do uso dos serviços de rede.

A ISO 27701 estabelece que a empresa deve assegurar que os usuários com acesso à dados pessoais estejam sujeitos a um acordo obrigatório de confidencialidade. Esse acordo pode ser parte de um contrato ou, de forma separada, especifique por quanto tempo convém que as obrigações sejam cumpridas.

8.4.1.1 OAS – Gerenciamento de acesso do usuário

A organização deve assegurar o acesso de usuário autorizado e prevenir acesso não autorizado a sistemas, serviços e informações.

Para o registro de usuários, um processo formal deve ser implementado, bem como um processo para o cancelamento de usuários. Como boa prática exposta no item 9.2.1 da ISO 27002, o processo para gerenciar o ID de usuário deve incluir:

a) Uso de ID de usuário único, para permitir relacionar os usuários às suas responsabilidades e ações. O uso compartilhado somente será permitido onde são necessários por razões operacionais ou de negócios, sendo esse compartilhamento documentado;
b) Imediata remoção ou desabilitação do ID de usuário que tenham deixado a organização;

Ao atribuir ou revogar direitos de acesso à IDs de usuário, o processo deve incluir:

a) Verificação de que existe autorização do proprietário do sistema ou serviço de informação para o uso;
b) Verificação de que o nível de acesso concedido é apropriado às políticas de acesso;
c) Deve existir um registro central de direitos de acesso concedido ao ID de usuário para acessar serviços e sistemas de informação;
d) Adaptação dos direitos de acesso dos usuários que tenham mudado de função ou atividades e imediata remoção ou bloqueio dos direitos de acesso dos usuários que deixaram a organização.

8.4.2 OAS – Gerenciamento de senhas

A autenticação de acesso a informações deve ocorrer por meio de senha, com política de renovação definida. A concessão de senha deve ser controlada por meio de um processo de gerenciamento formal. Para isso, no item 9.2.4 da ISO 27702 são dispostas as seguintes diretrizes para implementação:

a) Solicitar aos usuários a assinatura de uma declaração de confidencialidade das senhas e para manter as senhas de grupos de trabalho exclusivamente com os membros do grupo. Esta declaração assinada pode ser incluída nos termos e condições de contratação;

b) Garantir que nos casos em que os usuários necessitam manter suas próprias senhas, que seja fornecida uma informação de autenticação secreta temporária, onde o usuário deve alterá-la no primeiro uso;
c) Verificar a identidade de um usuário antes de fornecer uma senha, temporária, de substituição ou nova;
d) A senha temporária deve ser fornecida de maneira segura, evitando o uso de mensagens de correio eletrônico de terceiros ou desprotegido (texto claro);
e) A senha temporária deve ser única para uma pessoa e não deve ser fácil de ser adivinhada;
f) Os usuários devem acusar o recebimento da senha;
g) As senhas padronizadas devem ser alteradas logo após a instalação de sistemas ou *software*.

Os usuários devem ser orientados a seguir as práticas da organização quanto ao uso da senha. É responsabilidade do usuário a proteção das suas senhas, como disposto no item 9.3 da ISO 27702. Todos os usuários devem ser informados para:

a) Manter a confidencialidade da senha, garantindo que ela não seja divulgada para quaisquer outras partes, incluindo autoridades e liderança;
b) Evitar manter anotada as senhas (por exemplo, papel, arquivos ou dispositivos móveis), a menos que possa ser armazenada de forma segura e o método de armazenamento esteja aprovado (por exemplo, sistema de gerenciamento de senha);
c) Alterar a senha sempre que existir qualquer indicação de comprometimento do sistema ou da senha;
d) Selecionar senhas de qualidade, com um tamanho mínimo que:
    a. Sejam fáceis de lembrar;
    b. Não baseadas em nada que alguém possa facilmente adivinhar ou obter usando informações relativas à pessoa (nomes, números de telefone, datas de aniversário);
    c. Não vulneráveis à ataques de dicionário;
    d. Isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos;
    e. Em caso de senha temporária, ela deve ser mudada no primeiro acesso.
e) Não compartilhar a senha;

f) Garantir adequada proteção de senhas quando são usadas em procedimentos automáticos de acesso e são armazenadas;
g) Não utilizar a mesma senha para uso com finalidades profissionais e pessoais.

8.5 OAS – Não conformidade e comunicação

Medidas devem ser adotadas a fim de identificar violações à política de segurança da informação da organização. Segundo o item 10.1 da ISO 27001, quando uma não conformidade ocorre a organização deve reagir à não conformidade, tomar ações para corrigi-la e tratar com as consequências. Também deve avaliar as necessidades de ações para eliminar as causas da não conformidade, com análise crítica, determinando as causas do acontecimento e determinando se não conformidades similares existem ou podem potencialmente ocorrer, efetuando ações corretivas e alterações na política quando necessário.

8.5.1 OAS – Notificando fragilidades

Os usuários que usam serviços e sistemas de informação da empresa devem ser instruídos a notificar qualquer suspeita ou fragilidade da segurança da informação encontrada. Essas notificações devem ser relatadas à um ponto de contato previamente definido pela empresa de forma a prevenir incidentes de segurança da informação.

Conforme disposto no item 16.1.3 da ISO 27002, é importante notar que os usuários não devem tentar provar as fragilidades suspeitas, podendo ser interpretado como potencial mau uso do sistema e podendo causar danos ao serviço, resultando em responsabilidade legal para o usuário que afetou o sistema.

8.5.2 OAS – Avaliação e Resposta de Incidentes

Um ponto de contato definido pela empresa deve ser definido e será responsável pela avaliação, priorização e classificação de eventos e incidentes de segurança da informação. A priorização e classificação de incidentes podem ajudar a identificar o impacto e abrangência do incidente. Os resultados da avaliação devem ser registrados em detalhes com o propósito de verificação e referência futura.

Na ocorrência do incidente de segurança da informação, o incidente deve ser reportado para as pessoas relevantes dentro da organização e partes externas relevantes. O item 16.1.5 da ISO 27702 dispõe que a notificação deve incluir os seguintes itens:

a) Coleta de evidências, tão rápido quanto possível, logo após a ocorrência;
b) Condução de análise forense de segurança da informação;
c) Garantia de que todas as atividades de respostas envolvidas sejam adequadamente registradas para análise futura;
d) Comunicação da existência de incidente de segurança da informação ou qualquer detalhe relevante para pessoas internas ou externas, ou organizações que precisam tomar conhecimento;
e) Tratamento com as fragilidades de segurança da informação encontradas que causem ou contribuam para o incidente;
f) Sendo o incidente tratado de forma bem-sucedida, o mesmo deve ser encerrado e registrado formalmente.

Análises pós-incidente podem ser realizadas para identificar a fonte do incidente. O primeiro objetivo de resposta a incidente deve ser retornar ao nível de segurança normal e então iniciar qualquer recuperação que seja devida.

Um evento de segurança da informação pode envolver dados pessoais, sendo necessária análise crítica para verificação se houve a violação. Não necessariamente um evento resulta em uma probabilidade de acesso não autorizado à dados pessoais, isso pode incluir, mas não está limitado a *pings* e outros ataques de *broadcas*t a *firewalls*, varreduras de portas e tentativas de acessos malsucedidas, ataques de *denial of service* e *sniffing* de pacotes.

Na ocasião de violação de dados pessoais, a organização deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança da informação que possa acarretar risco ou dano relevante aos titulares. A comunicação deve ser feita em prazo razoável e, conforme a legislação, mencionar no mínimo:

I. A descrição da natureza dos dados pessoais afetados;
II. As informações sobre os titulares envolvidos;
III. A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
IV. Os riscos relacionados ao incidente;
V. Os motivos da demora, no caso de a comunicação não ter sido imediata;
VI. As medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Conforme a ISO 27701, em situação em que a violação de dados pessoais ocorreu, além do disposto pela LGPD, a organização também deve manter registro com informação suficiente para fornecer um relatório para propósitos forense contendo:

- Descrição do incidente;
- Período do tempo;
- Consequências do incidente;
- Nome do relator;
- Para quem o incidente foi reportado;
- Passos tomados para resolver incidentes;
- Se o incidente resultou em indisponibilidade, perda, divulgação ou alteração de dados pessoais.
- Descrição do dado pessoal comprometido, se conhecido;

8.5.3 OAS – Medidas Disciplinares

Para a obtenção da OEA, devem ser previstas medidas disciplinares aplicáveis aos casos de violação à política de segurança da informação. A empresa deve elaborar um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação. Para que isso ocorra, deve haver uma verificação prévia de que a violação da segurança da informação realmente ocorreu

A organização deve definir e aplicar procedimentos para a identificação, coleta, aquisição e preservação de informações que possam servir como evidências. A ISO 27702 no seu artigo 16.1.7 dispõe que os procedimentos devem levar em conta:

a) Cadeia de custódia;
b) Segurança da evidência;
c) Segurança das pessoas;
d) Papéis e responsabilidades das pessoas envolvidas;
e) Competência do pessoal;
f) Documentação;
g) Resumo do incidente.

O processo disciplinar formal deve assegurar um tratamento justo e correto aos funcionários que sejam suspeitos de cometer violações de segurança da informação. Deve

levar em consideração a gravidade da violação e seu impacto no negócio, a reincidência ou não do delito, treinamento do infrator, as legislações relevantes e os contratos do negócio.

8.6 OAS – Tratamento de Dados Pessoais

A organização deve assegurar que os titulares de dados pessoais entendam o propósito para os quais seus dados serão tratados. A empresa deve comunicar e documentar isto para os titulares, sem uma clara declaração do propósito de tratamento, não é possível que o consentimento seja colhido adequadamente.

Segundo a LGPD, as atividades de tratamento de dados pessoais pelas empresas deverão observar a boa-fé e os seguintes princípios:

I. Finalidade: O tratamento será realizado para propósitos legítimos, específicos, explícitos e informados ao titular;
II. Adequação: Compatibilidade do tratamento com as finalidades informadas ao titular;
III. Necessidade: Limitação do tratamento ao mínimo necessário, adequado e relevante para a realização das suas finalidades. A organização deve definir e documentar os objetivos da minimização dos dados e quais mecanismos (exemplo: anonimização) são usados para atender os objetivos;
IV. Livre acesso: Consulta facilitada aos titulares de dados pessoais sobre a forma, duração do tratamento e integridade dos seus dados;
V. Qualidade dos dados: Garantir aos titulares a precisão dos dados de acordo com a necessidade e finalidade do tratamento. A empresa deve implementar mecanismos e políticas para minimizar a imprecisão dos dados tratados. Também deve existir procedimentos para responder à casos de imprecisão do dado pessoal, esse procedimento pode estar incluído na informação documentada (exemplo: configurações de sistemas técnicos).
VI. Transparência: Garantir aos titulares informações claras e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento;
VII. Segurança: Utilização de medidas técnicas e administrativas aptas a proteção de dados pessoais de acessos não autorizados ou situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII. Prevenção: A empresa deve adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX. Não discriminação: Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X. Responsabilização: O agente de tratamento de dados deve adotar medidas eficazes e capazes de comprovar o cumprimento das normas de proteção dos dados pessoais e sua eficácia.

8.6.1 OAS – Agentes de Tratamento

A empresa deve nomear os agentes de tratamento de dados pessoais, sendo eles o Controlador e o Operador.

Para a LGPD, o Controlador é pessoa natural ou jurídica, a quem competem as decisões referentes ao tratamento de dados pessoais. O Operador é também pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador. O Artigo 39 da LGPD ainda destaca que o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador.

Perante a LGPD, o controlador ou operador que durante o tratamento de dados pessoais causar dano patrimonial, moral, individual ou coletivo, em violação à legislação vigente, é obrigado a repará-lo.

Os agentes devem manter registro das operações de tratamento de dados pessoais realizados. A ISO 27701 propõe no item 7.2.8 que a empresa pode implementar um inventário ou lista das atividades de tratamento que são realizados. Essa lista pode incluir:

- Tipo de tratamento;
- Propósitos para o tratamento;
- Descrição das categorias de dados pessoais;
- Categorias de destinatário para quem o dado será divulgado, incluindo destinatários de outros países ou organizações internacionais. Quaisquer divulgações adicionais para terceiros, como as que surgem de investigações legais ou auditorias externas devem ser registradas;
- Avaliação de Impacto de Privacidade (conforme Item 6.3);

Em seu artigo 41, a LGPD dispõe que o controlador deverá indicar o encarregado pelo tratamento de dados pessoais, sua identidade e informações para contato devem ser divulgadas publicamente e preferencialmente no site da empresa.

Entre suas atribuições dispostas na LGPD, o encarregado ficará responsável por aceitar reclamações e comunicações dos titulares de dados pessoais e da autoridade nacional e

tomar as providências cabíveis. É papel do encarregado orientar os funcionários e terceiros a respeito das boas práticas em relação à proteção dos dados pessoais.

A pessoa encarregada deve ser independente e deve reportar diretamente à alta direção para assegurar uma efetiva gestão de riscos de privacidade. Deve estar envolvida na gestão de todas as questões pertinente ao tratamento de dados e deve ter alto conhecimento sobre a LGPD.

8.6.2 OAS – Consentimento

Uma das hipóteses para o tratamento de dados pessoais segundo Lei Geral de Proteção de Dados Pessoais é que o tratamento de dados pessoais deverá ser realizado mediante o fornecimento de consentimento pelo titular.

A empresa deve determinar um processo pelo qual possa demonstrar quando e como o consentimento para o tratamento de dados pessoais foram obtidos dos titulares. A organização deve deixar clara a necessidade para a obtenção do consentimento e os requisitos para obter o consentimento.

O item 7.2.4 da ISO 27701 discorre que a organização deve obter e registrar os consentimentos dos titulares de dados pessoais de forma que, em caso de solicitação, seja possível fornecer detalhes do consentimento fornecido (exemplo: o tempo em que o consentimento foi fornecido, identificação do titular e a declaração de consentimento).

Antes de obter o consentimento, a empresa deve fornecer aos titulares de dados pessoais as informações que identifiquem o controlador de dados pessoais e descrevam o tratamento de seus dados pessoais, de forma clara e facilmente acessível, usando uma linguagem curta e clara, como apropriado ao público-alvo. A ISO 27701 dispõe que a informação a ser fornecida aos titulares de dados pessoais pode tomar o formato de uma notícia, podendo conter as seguintes informações:

- Informação sobre o propósito do tratamento;
- Detalhes do contato para o controlador de dados pessoais;
- Informação sobre as bases legais do tratamento;
- Informação sobre como o titular pode cancelar um consentimento;
- Informação sobre transferência de dados pessoais;
- Informação sobre o direito de apresentar uma reclamação e como apresentá-la;

8.6.3 OAS – Avaliação de Impacto de Privacidade

A organização deve aplicar o processo de avaliação de riscos de privacidade para identificar os riscos relativos ao tratamento de dados pessoais. A empresa deve assegurar que ao longo de todos os processos de avaliação de riscos que a relação entre a segurança da informação e a proteção de dados pessoais seja adequadamente gerenciada.

O tratamento de dados pessoais gera riscos para os titulares. Estes riscos devem ser avaliados por meio de uma avaliação de impacto de privacidade, determinando os elementos que são necessários para uma avaliação de impacto de privacidade completo. O item 7.2.5 da ISO 27701 dispõe os elementos possíveis a serem avaliados:

- Tipos de dados pessoais tratados;
- Armazenamento de dados pessoais;
- Transferência de dados pessoais;
- Diagramas de fluxos de dados e mapa de dados;
- Lista de atividades de tratamento de dados pessoais;

8.6.4 OAS – Consulta, Cópia, Correção e Exclusão de Dados Pessoais

A empresa deve implementar mecanismos para que os titulares de dados pessoais acessem, corrijam ou excluam seus dados pessoais quando solicitado e sem atraso indevido, conforme proposto no item 7.3.6 da ISO 27701. A organização deve definir um tempo de resposta para que a solicitação seja tratada dentro do prazo definido.

Toda e qualquer correção ou exclusão aplicada devem ser disseminadas por todo o sistema ou para os usuários autorizados e para terceiros aos quais os dados pessoais foram transferidos.

Ao ser solicitada a confirmação de existência ou acesso a dados pessoais a organização pode fornecer uma cópia do dado pessoal que é tratado em um formato estruturado acessível pelo titular de dados pessoais. A empresa deve assegurar que quaisquer cópias de dados fornecidas estejam especificamente relacionadas com aquele titular de dados pessoais. Em caso de o dado pessoal já tiver sido excluído, convém que o controlador informe ao titular que o dado requerido não consta mais nos registros.

8.7 OAS - Relação OEA x LGPD x ISO

A seguir é apresentado um quadro de relações entre os módulos do framework em relação aos itens exigidos na OEA, os artigos atingidos diretamente na LGPD e os controles propostos na família de normas ISO 27000. Essa tabela foi elaborada com objetivo de facilitar a compreensão sobre o framework desenvolvido em relação suas exigências à serem atendidas e instruções normativas norteadoras para o seu desenvolvimento.

Quadro 7 – Quadro Comparativo OAS x OEA x LGPD x ISO

OAS FRAMEWORK	DESCRIÇÃO	OEA	LGPD	ISO 27001	ISO 27002	ISO 27701
1.0	Política de Segurança da Informação	Item 1.2.2.2. D	Art. 46 Art. 47 Art. 48 Art. 49 Art. 50	Item 5.2	Cap. 5	
2.0	Política de Backup	Item 1.2.2.2. G	Art. 46		Item 12.3.1	Item 6.9.3
3.0	Política de Privacidade		Art. 7 Art. 8 Art. 9			Item 6.2.1.1
4.0	Restrição à Informação	Item 1.2.2.2. A Item 1.2.2.2. B Item 1.2.2.2. C	Art. 46 Art. 47		Cap. 9	Item 6.10.2.4
5.0	Não Conformidade e Comunicação	Item 1.2.2.2. E Item 1.2.2.2. F	Art. 48	Item 10.1	Item 7.2.3 Cap. 16	Item 6.13.1.5
6.0	Tratamento de Dados Pessoais		Art. 5 Art. 6 Art. 7		Item 6.1	Item 6.3.1.1 Item 7.1 Item 7.2

			Art. 8			Item 7.2.3
			Art. 9			Item 7.2.4
			Art. 10			Item 7.2.5
			Art. 11			Item 7.2.8
			Art. 15			Item 7.3.3
			Art. 18			Item 7.3.4
			Art. 19			Item 7.3.6
			Art. 37			Item 7.3.8
			Art. 38			Item 7.4.1
			Art. 39			Item 7.4.3
			Art. 41			Item 7.4.4
			Art. 42			Item 8.5.3

Fonte: Elaborado pelo Autor

Nesse capítulo foi apresentado o OAS Framework, um artefato cujo objetivo é facilitar a adesão das empresas de comércio exterior à certificação OEA, no que tange à gestão da segurança da informação exigida pela certificadora Receita Federal. O framework também propôs controles para que a empresa obtenha aderência com os requisitos exigidos pela LGPD. No capítulo seguinte será apresentado o modelo de implementação do OAS Framework nas empresas.

9 IMPLEMENTAÇÃO DO FRAMEWORK

A proposta inicial deste trabalho foi de além de criar um framework de segurança da informação aderente com a certificação OEA e a adequação à LGPD, criar um modelo de maturidade baseado no COBIT 5 onde a organização consiga mensurar o nível de adequação à legislação vigente e à certificação requerida. No entanto, durante o levantamento de requisitos e definição de critérios para a criação do framework, ficou evidente a necessidade de todos os processos referentes à tratamento de dados pessoais e requisitos da OEA exigidos serem cumpridos na integra pela organização, para que seja possível dar início no processo de homologação.

As políticas de segurança da informação e privacidade de dados pessoais devem ser disseminadas nas organizações adotantes do framework, de forma a garantir a proteção dos serviços, dados e evitar sanções administrativas previstas na legislação e perda de confiança no mercado.

Exposto isso, o modelo da capacidade proposto pela COBIT 5 não se adequa as necessidades do OAS Framework, visto que todos os módulos devem ser cumpridos de forma integral pelas empresas, não havendo brechas para um processo incompleto ou que não seja otimizado pela organização. Os riscos de implementar os controles de forma parcial ou ineficiente incluem, mas não se limitam à:

- Falha na obtenção da certificação OEA para empresas que a buscam;
- Perda da certificação OEA para empresas já certificadas;
- Advertência ou multa aplicadas pela autoridade nacional;
- Suspensão do exercício da atividade de tratamento de dados;

Mesmo que um modelo de maturidade não seja implementado, deve-se notar que nenhuma organização implementará qualquer framework ou sistema de gestão de segurança da informação repentinamente. Conforme a ISO 27001, o estabelecimento e a implementação de controles de segurança da informação devem preservar a confidencialidade, integridade e disponibilidade da informação, assim, essa mudança requer esforço da organização e deve ser feito de modo gradativo.

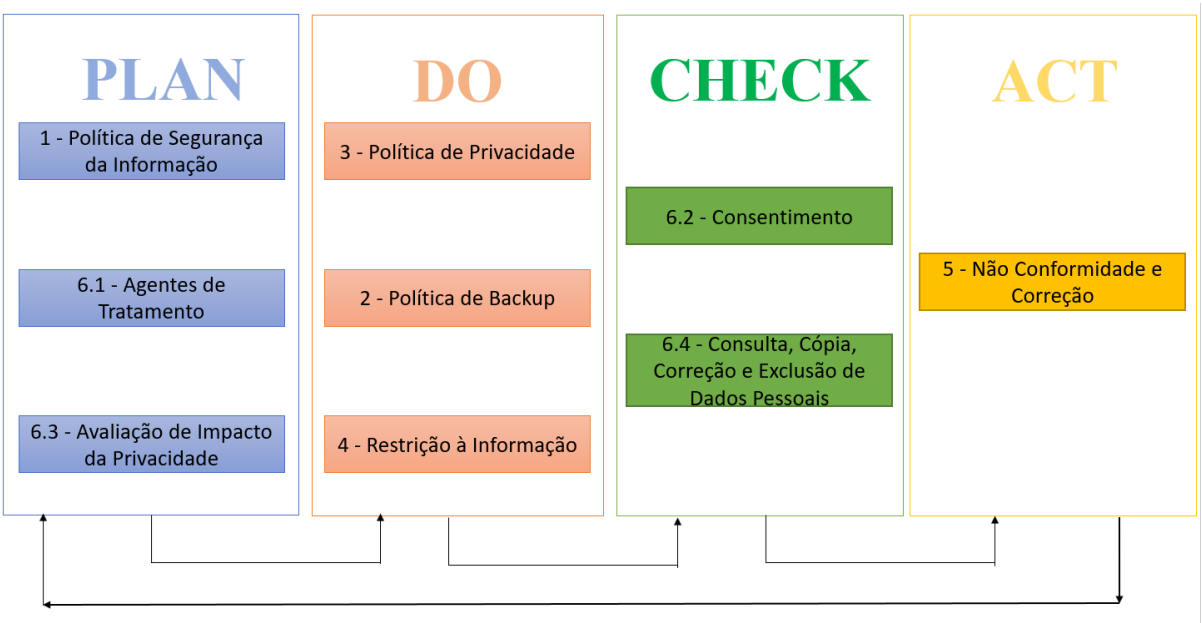
Pensando na melhoria contínua do processo e sua qualidade, para a implementação do OAS Framework é proposto que a implementação seja baseada no ciclo PDCA. Conforme destacado no capítulo referente à ISO 27001, o ciclo PDCA é um método interativo de controle e melhoria contínua, permitindo que as organizações melhorem os processos de forma contínua.

PACHECO *et al.* (2012) destacam que como pode ser observado na nomenclatura, o ciclo está dividido em 4 fases:

- Plan (Planejar): Estabelecimento de um plano de ações, definindo estratégias e objetivos;
- Do (Executar): Execução do que foi planejado;
- Check (Checar): Checar comparando os dados obtidos na execução com o que foi proposto no plano se os resultados foram atingidos;
- Act (Agir): Fazer as correções necessárias com o intuito de evitar que a repetição do problema venha a ocorrer.

Assim, os módulos do Framework foram divididos conforme as quatro fases do ciclo PDCA expostos na imagem abaixo:

Figura 11 – Ciclo PDCA no OAS Framework



Fonte: Elaborado pelo Autor

A fase do planejamento engloba os itens que serão a base para o processo de implementação do framework, os itens que são englobados na fase de execução devem ser realizados e seus resultados verificados na terceira fase, por fim, o ciclo termina na fase da ação, onde as correções necessárias devem ser executadas. Concluído esse ciclo, um novo ciclo é gerado com as modificações aplicadas visando o aperfeiçoamento dos processos.

9.1 Ciclo PDCA - Plan

A primeira fase do ciclo contém o módulo 1.0 do OAS Framework – Política da Segurança da Informação. A política da segurança da informação inclui os objetivos da segurança da informação e pode fornecer a estrutura para estabelecer os objetivos de segurança da informação, sendo a base de toda a implementação do Framework. Por conter muitas das diretrizes a serem seguidas no restante dos processos, esse item se encontra na fase de planejamento do ciclo.

No planejamento deve ser definido quem são os agentes de tratamento e qual é o seu papel dentro da organização, em especial na figura do papel do encarregado, cuja função é orientar os funcionários e terceiros a respeito das boas práticas em relação à proteção dos dados pessoais, cabendo assim a essa fase o item 6.1 – Agentes de Tratamento. O item 6.3 - Avaliação de Impacto de Privacidade está na fase de planejamento, visto que os dados devem ser mapeados para análise de risco de tratamento dos dados pessoais.

9.2 Ciclo PDCA - Do

Na Política de Privacidade está exposta a proposta da organização com o comprometimento para obter aderência com as legislações de dados pessoais, expondo as medidas aplicadas pela organização para obter a aderência. Essa política é apresentada para os usuários em busca do consentimento para o tratamento dos dados.

O módulo 2 - Política de Backup, contém as diretrizes efetuadas para que as informações relacionadas com as operações de comércio exterior sejam armazenadas de forma que possibilite sua restauração. Por se tratar de uma política de execução obrigatória para obtenção da OEA, se encontra no ciclo Do.

A restrição à informação abordada no módulo 4, contém as ações para que todas as informações relacionadas com as operações de comércio e exterior e dados pessoais estejam protegidas contra acesso não autorizado e situações acidentais ou ilícitas de destruição, perda, alteração ou qualquer forma de tratamento ilícito, essas ações são fundamentais para a continuação do processo e por isso listadas no ciclo Do.

9.3 Ciclo PDCA - Check

A empresa deve checar se o consentimento está sendo estabelecido de forma transparente conforme política de privacidade e requisitos estabelecidos no item 6.2 – Consentimento. Conforme explicado no item citado, a empresa deve determinar um processo pelo qual possa demonstrar quando e como o consentimento para o tratamento de dados pessoais foram obtidos dos titulares. A organização deve deixar clara a necessidade para a obtenção do consentimento e os requisitos para obter o consentimento.

As solicitações de consulta se enquadram no ciclo Check, conforme item 6.4, a empresa deve implementar mecanismos para que os titulares de dados pessoais consultem, corrijam ou excluam seus dados pessoais quando solicitado e sem atraso indevido.

9.4 Ciclo PDCA - Act

No ciclo Act, procura-se realizar correções necessárias com o intuito de evitar que a repetição do problema venha a ocorrer. Assim, medidas devem ser adotadas a fim de identificar violações à política de segurança da informação da organização.

Quando uma não conformidade ocorre a organização deve reagir à não conformidade, tomando ações para corrigi-la e tratar com as consequências, sendo esses os itens abordados pelo módulo 5 – Não Conformidade e Correção.

O módulo também discorre que também deve ser avaliado as necessidades de ações para eliminar as causas da não conformidade, com análise crítica, determinando as causas do acontecimento e determinando se não conformidades similares existem ou podem potencialmente ocorrer, efetuando ações corretivas e alterações na política quando necessário.

Após concluído esse ciclo, um novo ciclo recomeça com as modificações necessárias para a melhoria do processo.

10 AVALIAÇÃO QUALITATIVA

Tendo sido criado o Framework conforme exposto no capítulo 8 e conforme os objetivos propostos dentro do presente trabalho, se faz necessária a validação do artefato desenvolvido. Para isso, o framework foi apresentado para especialistas dentro da área de TI e comércio exterior com o propósito de validar, criticar e contribuir com o artefato gerado.

A escolha dos entrevistados foi feita através de contatos comerciais já estabelecidos com o entrevistador, também foram procuradas pessoas interessadas a contribuir com a avaliação através da rede social LinkedIn, mas não houve interessados em participar da pesquisa. A composição da avaliação aplicada pode ser consultada no Apêndice B.

A ferramenta utilizada para a realização da avaliação foi o Google Formulários, sendo o questionário enviado junto do Framework e sua proposta de implementação. O documento foi enviado por e-mail, contendo orientações sobre o preenchimento da avaliação e o e-mail do pesquisador foi deixado à disposição para resolução de quaisquer dúvidas possíveis a respeito do OAS Framework e da avaliação qualitativa. Junto à avaliação, os entrevistados receberam o termo de consentimento livre e esclarecido descrevendo o objetivo da pesquisa e esclarecendo o compromisso com a anonimização das informações comerciais envolvidas. O termo está exposto no Apêndice A do trabalho.

O formulário ficou disponível durante 14 dias, período aberto a partir do primeiro aceite de um especialista, até a data limite para a realização da avaliação estipulada no cronograma do entrevistador para essa pesquisa. O questionário contém sete (07) questões a respeito do entrevistado e a empresa de atuação e oito (08) questões sobre a percepção sobre o framework gerado, onde o entrevistado pôde através da Escala de Likert de cinco (05) pontos validar o OAS Framework.

Segundo JÚNIOR; COSTA (2014) a escala de verificação de Likert consiste em tomar um construto e desenvolver um conjunto de afirmações relacionadas à sua definição, onde os respondentes emitirão seu grau de concordância. Ainda segundo os autores, a grande vantagem da escala de Likert é sua facilidade de manuseio, pois é fácil a um pesquisado emitir um grau de concordância sobre uma afirmação qualquer.

Decorrido o prazo máximo para recebimento das respostas do questionário, a avaliação qualitativa foi finalizada e seus dados foram compilados. Os resultados obtidos estão expostos abaixo.

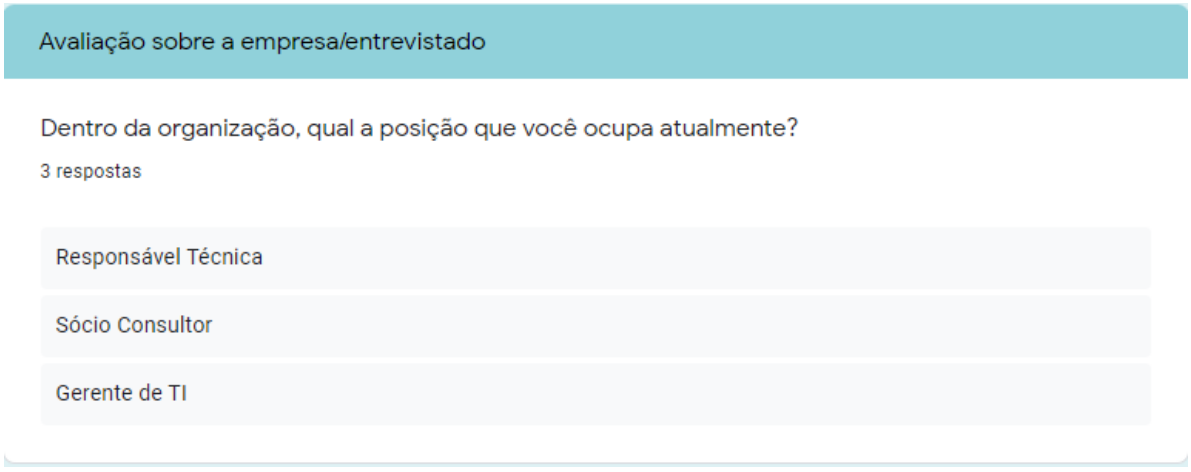
10.1 Resultados

Com base na coleta de dados, os resultados da avaliação foram planilhados, analisados e os resultados são apresentados e discutidos a seguir. Três entrevistados leram o framework desenvolvido e responderam o questionário. Seus nomes e empresas a quais representam serão omitidos para garantir o sigilo das informações comerciais em que estão envolvidos, conforme o Termo de Consentimento Livre e Esclarecido, conforme apresentado no apêndice A.

As primeiras questões da avaliação buscam traçar o perfil do entrevistado em relação à sua empresa, situação atual em relação com a adesão à OEA e LGPD e o conhecimento que eles possuem sobre os dois temas. A escala de Likert nos questionamentos dessa seção vão de 1 a 5, sendo a escala 1 como “Pouco Conhecimento” e a escala 5 como “Bom Conhecimento”.

A primeira questão busca entender a posição ocupada pelo entrevistado e que o credencia a participar dessa pesquisa. Conforme ilustrado pela figura 12, responderam à avaliação uma Responsável Técnica, um Sócio Consultor e um Gerente de TI. Todos os entrevistados citados já atuaram diretamente em implementações de certificação OEA e adequação à LGPD em suas empresas, o que os credencia para realizar a avaliação do OAS Framework.

Figura 12 – Cargo ocupado pelo entrevistado

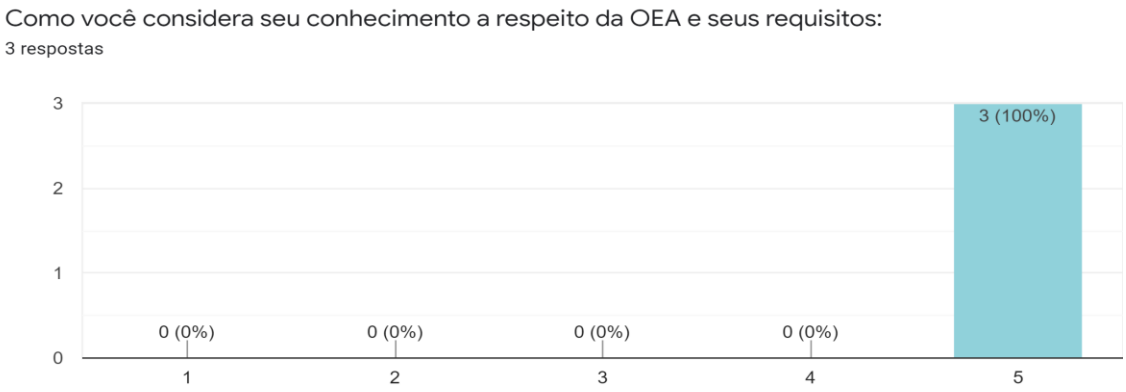


Fonte: Elaborado pelo Autor

A segunda questão propõe fundamentar o conhecimento do entrevistado a respeito da OEA e seus requisitos. Conforme o Gráfico 1 demonstra, todos marcaram 5 pontos assim,

afirmam possuir bom conhecimento sobre a OEA, sendo capazes de avaliar plenamente os controles desenvolvidos no framework.

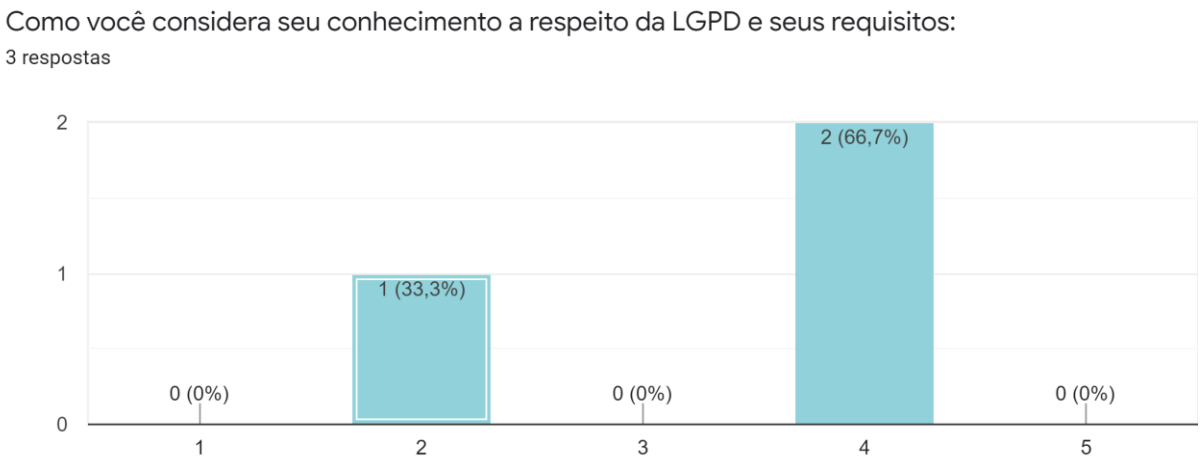
Gráfico 1 – Conhecimento sobre a OEA



Fonte: Elaborado pelo Autor

O conhecimento sobre a LGPD e seus requisitos é o tema do terceiro questionamento da avaliação. Esse questionamento busca entender o conhecimento do entrevistado em relação à LGPD. Dentro da escala de Likert, um entrevistado marcou 2 pontos e outros dois entrevistados marcaram 4 pontos, assinalando conhecer um razoável conhecimento sobre a legislação de proteção de dados, conforme o Gráfico 2 expõe abaixo:

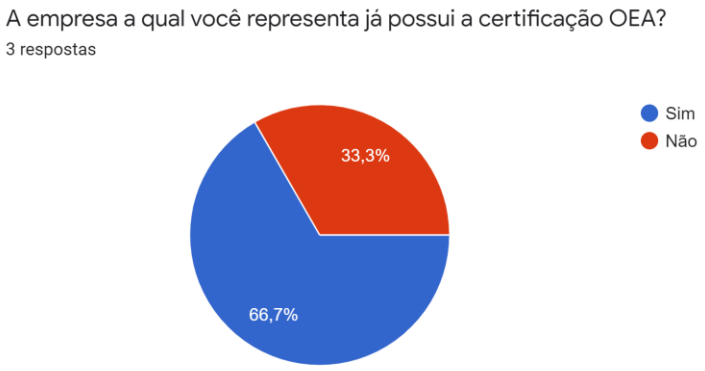
Gráfico 2 – Conhecimento sobre a LGPD



Fonte: Elaborado pelo Autor

O quarto questionamento propõe entender se a empresa a qual o entrevistado representa possui ou não a certificação OEA. O Gráfico 3 nos mostra que a empresa de 66,7% dos entrevistados possui a certificação, enquanto a empresa de 33,3% dos entrevistados não é certificada OEA. Conforme será visto no Gráfico 4, a empresa do entrevistado que não possui a certificação OEA não é elegível para obtê-la, mas tem ligação direta com a certificação.

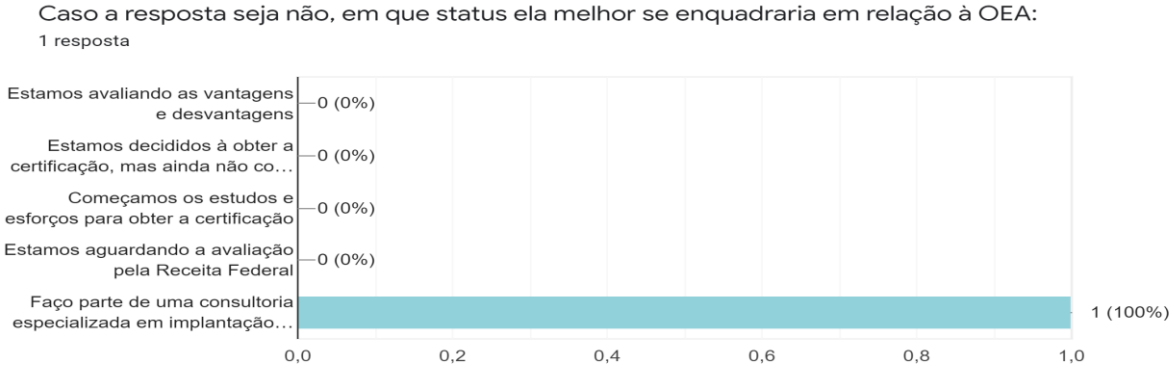
Gráfico 3 – Certificação OEA por empresa



Fonte: Elaborado pelo Autor

Ainda relacionado com o quarto questionamento, buscou-se entender o status das empresas em relação à OEA. Em caso da não obtenção da certificação buscou-se entender o contexto e status da empresa. Conforme o Gráfico 4, o representante da empresa sem a certificação respondeu “Faço parte de uma consultoria especializada em implantação do programa OEA e normas certificáveis”. Dessa forma, demonstra que possui conhecimentos relacionados à OEA e diversas normas.

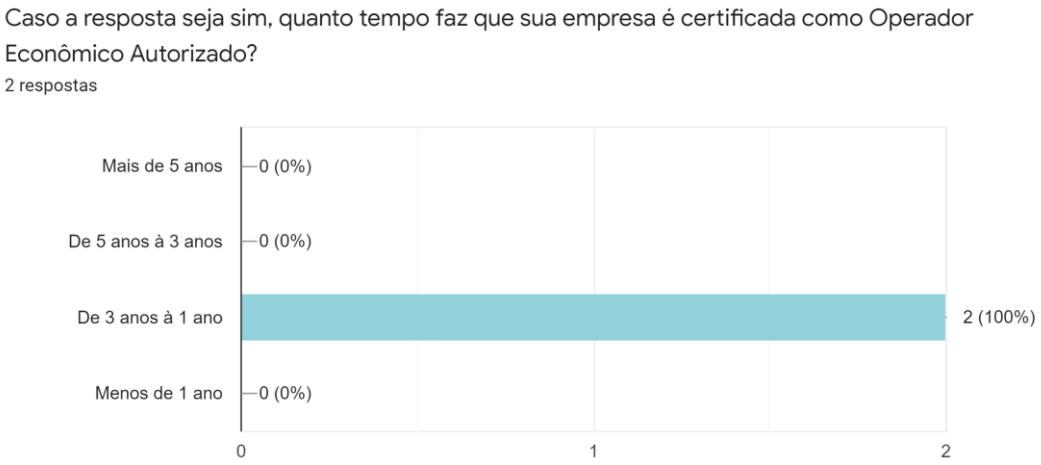
Gráfico 4 – Status da empresa em relação à OEA



Fonte: Elaborado pelo Autor

Em caso de resposta positiva em relação à empresa ter certificação de operador econômico autorizado, foi perguntado para os entrevistados a quanto tempo a empresa possuía a certificação. Foi observado que os outros dois entrevistados representam empresas que detém a certificação no período de 3 anos a 1 ano. O Gráfico 5 expõe os resultados:

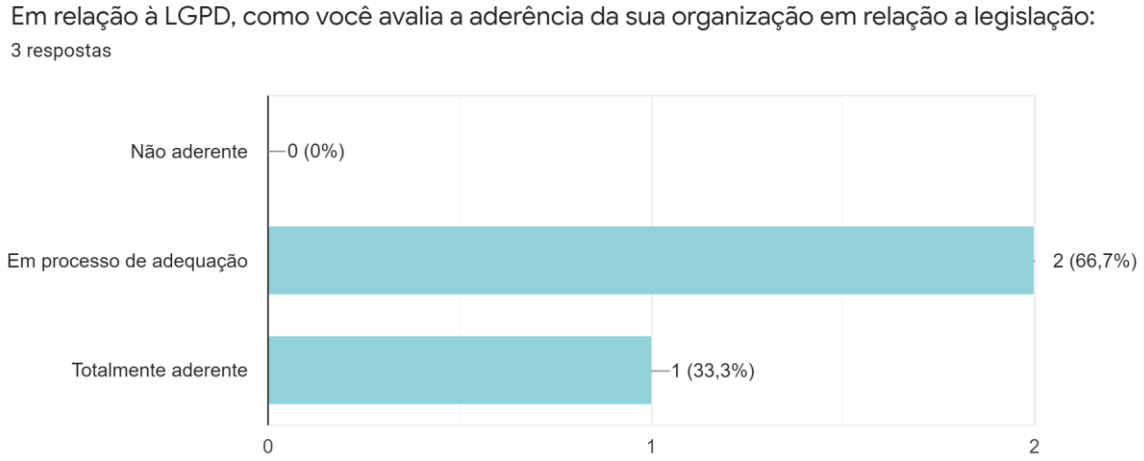
Gráfico 5 – Tempo de credenciamento OEA



Fonte: Elaborado pelo Autor

A última questão da seção de perguntas sobre a empresa e entrevistado propõe avaliar a aderência da organização dos especialistas com a LGPD. Verificou-se que 66,7% das empresas estão em processo de adequação, enquanto 33,3% se consideram totalmente aderentes a legislação proposta. Esse resultado mostra que os entrevistados atuam em empresas onde a aderência à LGPD é um tópico relevante. Abaixo, o Gráfico 6 demonstra as respostas ao questionamento proposto:

Gráfico 6 – Aderência da empresa em relação à LGPD

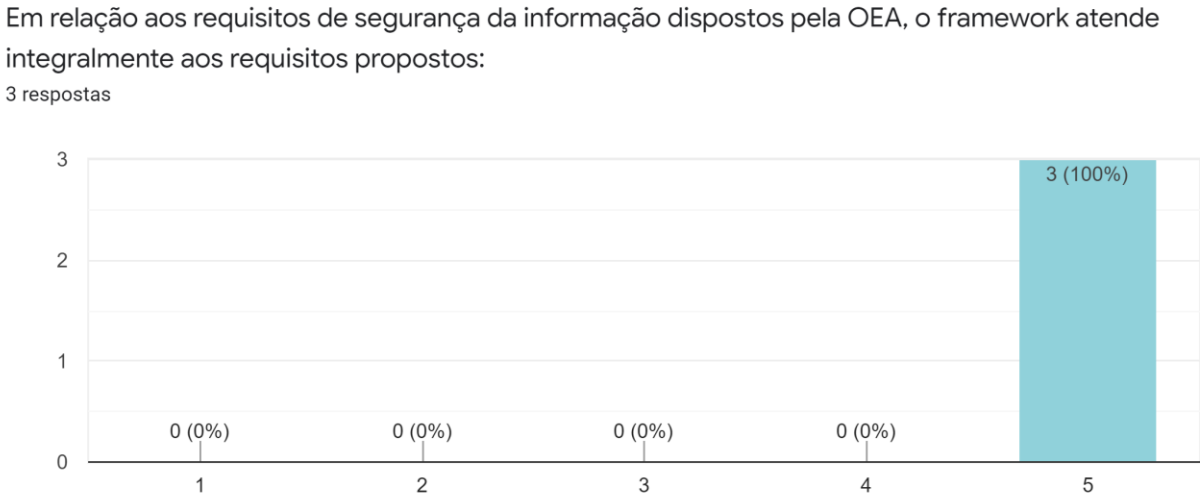


Fonte: Elaborado pelo Autor

A segunda seção do questionário contém perguntas sobre a percepção dos especialistas quanto ao OAS Framework. A escala de Likert nos questionamentos dessa seção vão de 1 a 5, sendo a escala 1 como “Discordo Totalmente” e a escala 5 como “Concordo Totalmente”.

A primeira questão busca entender a opinião dos especialistas se o framework atende integralmente os requisitos de segurança da informação dispostos na OEA. Esse questionamento é relevante dada a importância da segurança da informação no escopo da OEA, sem cumprimento pleno dos requisitos não há possibilidade de a empresa candidata da certificação seguir com o processo de validação junto à Receita Federal Brasileira. Conforme o Gráfico 7 ilustrado abaixo, os entrevistados concordam que o framework cumpre ao requisito de segurança da informação proposto:

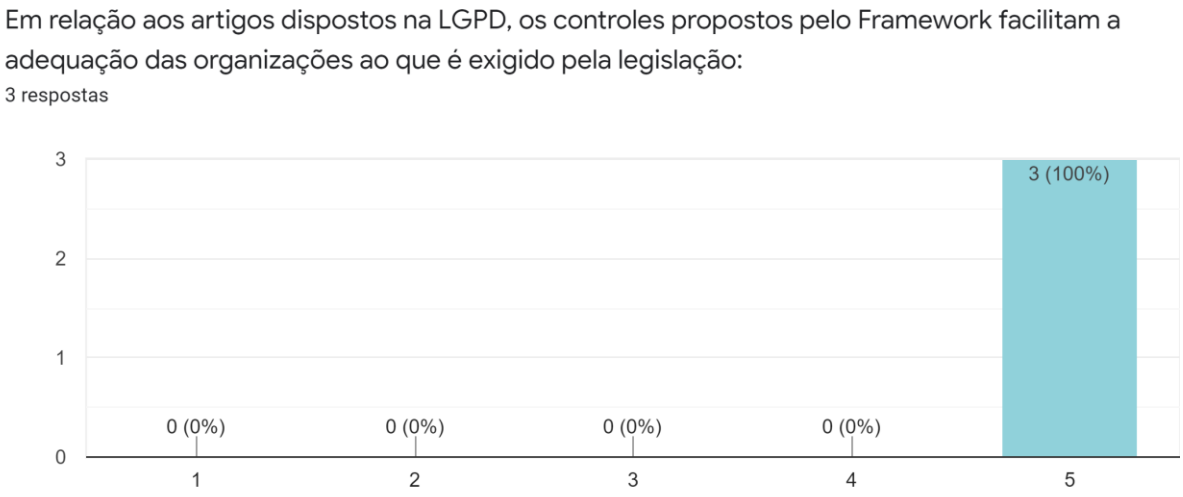
Gráfico 7 – Requisitos de Segurança da Informação do Framework na OEA



Fonte: Elaborado pelo Autor

O segundo questionamento propõe avaliar se os controles propostos pelo Framework facilitam a adequação das organizações ao que é exigido pela LGPD, sendo esse um dos objetivos fundamentais do OAS Framework. O Gráfico 8 nos mostra que segundo os entrevistados, todos concordam que o OAS Framework facilita a adequação exigida.

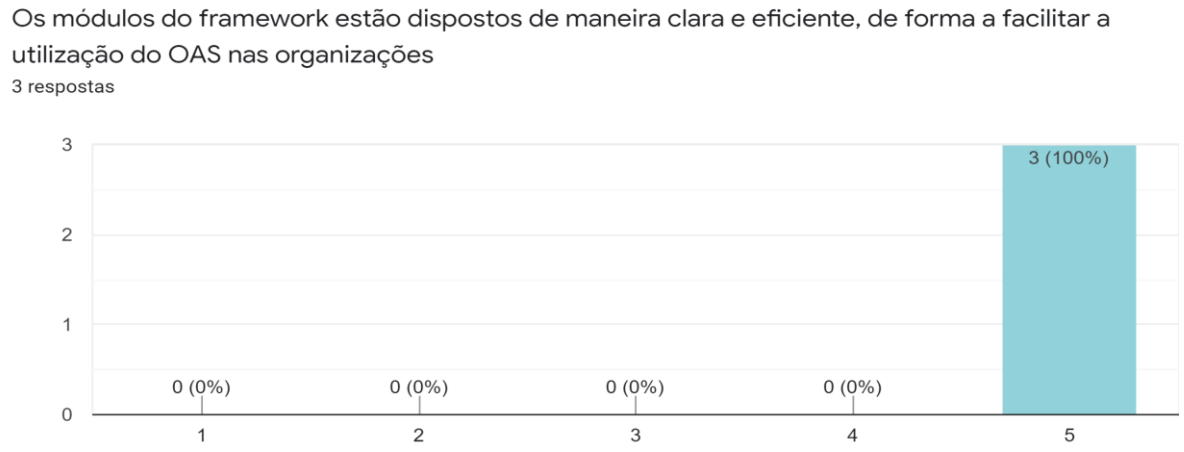
Gráfico 8 – Facilitação de adequação à LGPD pelo OAS Framework



Fonte: Elaborado pelo Autor

A terceira pergunta busca a percepção dos entrevistados se os módulos do framework estão dispostos de maneira clara e eficiente, facilitando a utilização do OAS. Neste questionamento, busca-se entender se a estrutura do framework está disposto de forma eficiente. Conforme pode ser observado no Gráfico 9, todos os entrevistados concordam totalmente que os módulos do OAS estão dispostos de maneira concisa.

Gráfico 9 – Disposição dos módulos do OAS Framework

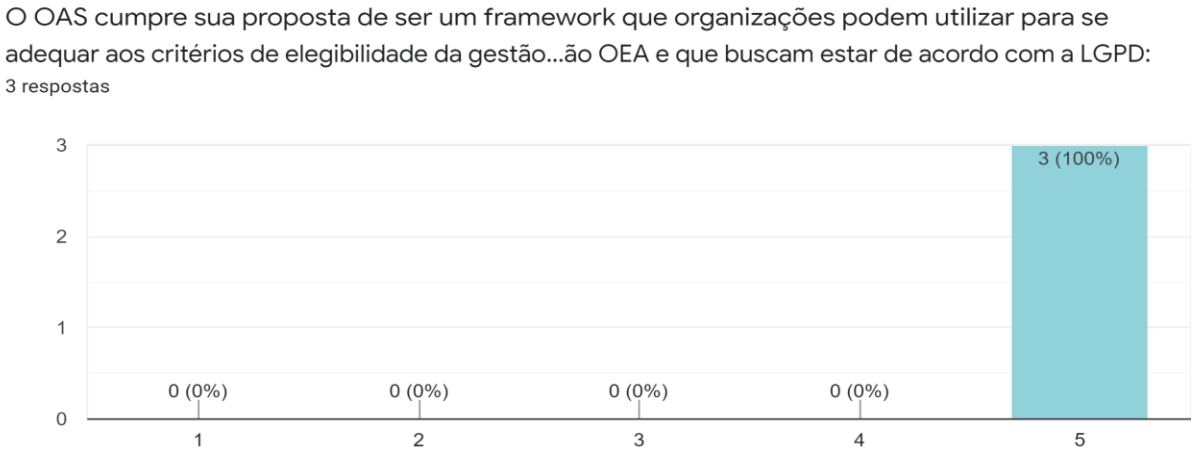


Fonte: Elaborado pelo Autor

No quarto questionamento realizado buscou-se entender se na opinião dos entrevistados, a proposta do OAS de ser um framework que organizações podem utilizar para se adequar aos critérios de elegibilidade da gestão da informação que compreendem aos requisitos de segurança da informação para obter a certificação OEA e que buscam estar de acordo com a LGPD foi atendida.

Essa avaliação também busca ter a constatação pelos especialistas de que essa proposta inicial do framework foi atingida de forma aceitável, Todos os entrevistados concordaram que a proposta do OAS Framework foi cumprida, conforme exposto pelo Gráfico 10.

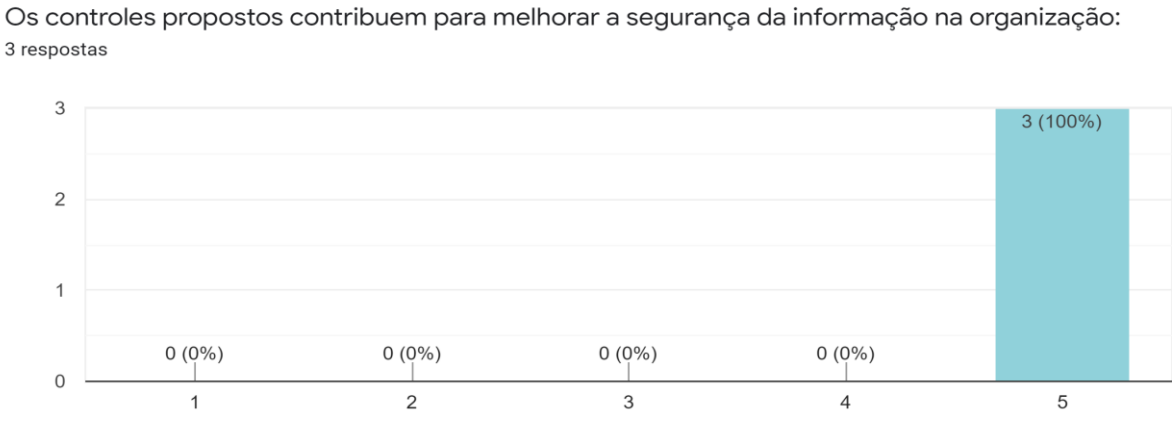
Gráfico 10 – O OAS Framework cumpre sua proposta de utilização



Fonte: Elaborado pelo Autor

Os entrevistados foram questionados se os controles propostos pelo OAS contribuem para melhorar a segurança da informação na empresa. Apesar de possuir um escopo de atuação bem definido, o OAS ainda é um framework de segurança da informação, assim, ter a capacidade de melhorar a segurança da informação na empresa é um item essencial e que deve ser avaliado. Conforme ilustrado pelo Gráfico 11, todas as respostas concordaram totalmente com a afirmação.

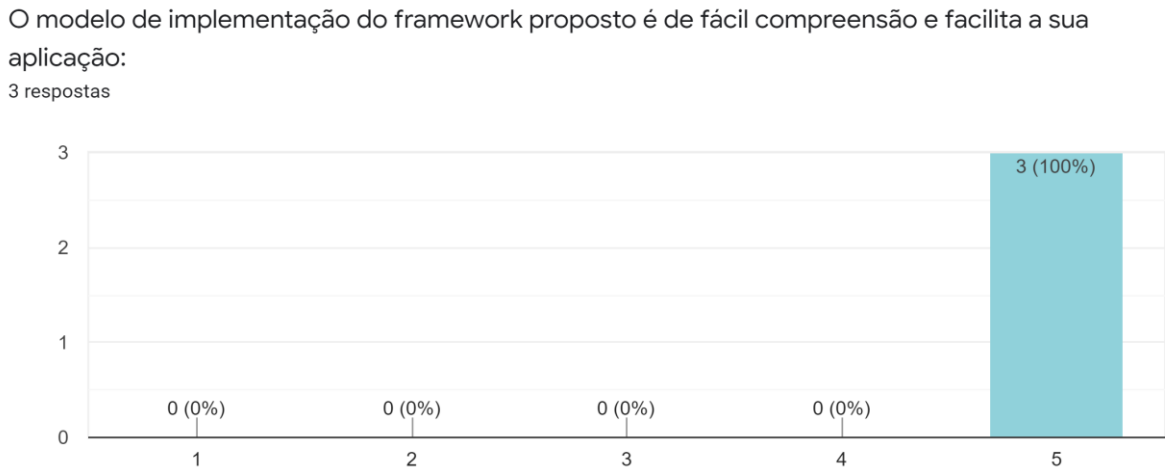
Gráfico 11 – O OAS contribui para melhorar a segurança da informação



Fonte: Elaborado pelo Autor

Os especialistas foram perguntados se o modelo de implementação do framework é de fácil compreensão e com aplicação facilitada, um requisito que deve ser atingido pelo OAS Framework. Como visto no gráfico 12, todos concordaram totalmente que o OAS possui um modelo de implementação de fácil compreensão e aplicabilidade.

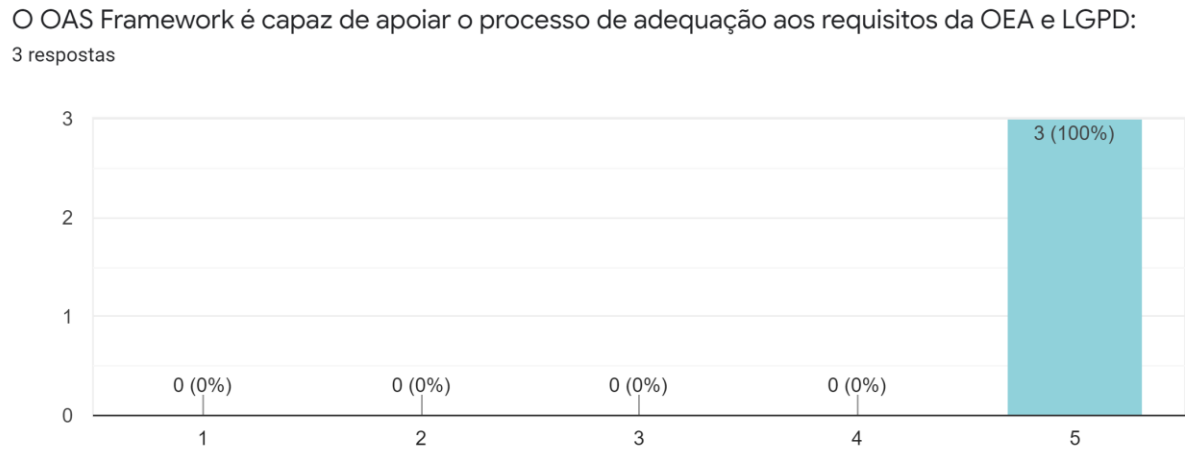
Gráfico 12 – O modelo de implementação do Framework é compreensivo e facilitado



Fonte: Elaborado pelo Autor

A penúltima pergunta busca saber se na opinião dos especialistas, o OAS é capaz de apoiar as organizações no processo de adequação aos requisitos da OEA e LGPD. A validação dessa afirmação é importante quando se visa a aplicação prática do framework proposto por empresas do comércio exterior. Todas as respostas concordam totalmente que sim, o OAS é capaz de apoiar o processo de adequação aos requisitos da OEA e LGPD, conforme ilustrado no Gráfico 13 abaixo:

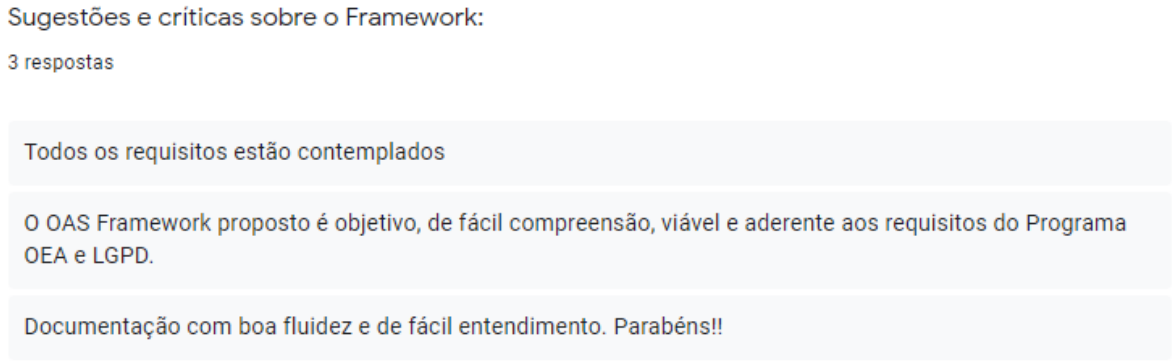
Gráfico 13 – O OAS é capaz de apoiar o processo de adequação aos requisitos da OEA e LGPD



Fonte: Elaborado pelo Autor

Por fim são solicitadas sugestões e críticas sobre o Framework, tendo os entrevistados dando as seguintes respostas, expostas na figura 13:

Figura 13 – Sugestões e críticas sobre o Framework



Fonte: Elaborado pelo Autor

Além da resposta dada na figura 13, um dos entrevistados optou por dar sugestões via ligação telefônica. Essas sugestões foram as seguintes:

I. No módulo 5.0 – Não conformidade e comunicação, a empresa pode buscar a causa raiz dos problemas apresentados;
II. Todo registro realizado deve ser formalizado com a alta direção da empresa;

III. Dentro do Ciclo PDCA, a obtenção do consentimento deve estar listado no ciclo “Do” e a Política de Backup deve estar listada no ciclo “Check”.

A respeito das sugestões dadas pelo entrevistado, o autor do presente estudo comprometeu-se a revisar os conceitos abordados para uma possível nova versão do OAS Framework e em caso de concordância, dar os créditos pertinentes pela observação realizada.

Com os resultados apresentados acima, é possível afirmar que para os especialistas em comércio exterior e gestão de TI, o OAS Framework atende integralmente as necessidades das empresas que buscam adequação aos requisitos da certificação OEA e aderência com a LGPD. Os resultados também evidenciam uma ampla aprovação sobre o modelo de implementação baseado no Ciclo PDCA.

11 CONCLUSÃO

No trabalho desenvolvido foram realizadas pesquisas para compreender o programa OEA Brasileiro, sua história, suas características e relevância no cenário do comércio exterior internacional. Também foi abordada a LGPD, com a história por trás da lei, os conceitos desenvolvidos e a sua importância no âmbito da proteção de dados pessoais.

Foi analisada também a família de normas ISO/IEC 27000, modelo de referência na gestão da segurança da informação, foram abordados os conceitos sobre cada norma, seus controles e contribuições.

Durante a pesquisa para o desenvolvimento do presente trabalho, foi observada a ausência de publicações relacionadas à certificação OEA no âmbito da implementação dos requisitos de segurança da informação necessários para estar aderente ao programa. Essa ausência de publicações foi um dos grandes desafios para a elaboração do OAS Framework, exigindo pesquisa profunda das normas de comércio exterior no Brasil e no mundo, para depois buscar-se entender a aplicabilidade da certificação OEA no contexto brasileiro atual.

A Lei Geral de Proteção de Dados é um tópico que vem sendo discutido nos últimos anos. A Lei aprovada em 2018 e em vigor desde 2020 tem se mostrado desafiadora para empresas e organizações públicas implementarem, visto que a lei não estabelece diretivas ou metodologias do que deve ser feito para que as empresas atinjam os objetivos expostos. É necessário destacar também que as punições previstas em caso de desacordo com a lei estão em vigor desde agosto de 2021.

Ao analisar os objetivos propostos para o presente trabalho e comparando-os com o trabalho desenvolvido é possível realizar algumas conclusões. O objetivo geral de "Desenvolver um framework de segurança da informação que auxilie organizações na adequação a Lei Geral de Proteção dos Dados (LGPD) e que tenha aderência com os critérios de elegibilidade exigidos pela certificação de Operador Econômico Autorizado (OEA)" foi plenamente cumprido, conforme o artefato desenvolvido no capítulo 8. O OAS Framework através dos seus 6 módulos tornou-se um artefato com potencial para ser utilizado para empresas do comércio exterior se adequarem a realidade brasileira e comercial atual, fato esse reforçado pela aprovação dos especialista, conforme apresentado no capítulo 10.

Ao verificar os objetivos específicos para o trabalho é possível verificar que foi desenvolvido estudo teórico sobre a certificação OEA, sobre a LGPD e leis de segurança da informação vigentes no Brasil, tal qual apresentado nos capítulos 3, 4 e 5. Esse estudo teórico

foi uma base fundamental para a análise dos requisitos que o Framework deveria atender, assim, cumprindo esse objetivo específico do trabalho.

Foi realizada pesquisa sobre os frameworks de segurança da informação existentes, tendo sido dado um foco muito relevante na família de normas da ISO/IEC 27000, exposta no capítulo 5, que serviu de base técnica para o desenvolvimento do framework.

Ao pensar o modelo inicial do framework a ser desenvolvido, foi proposta a elaboração de níveis de maturidade. Durante o desenvolvimento do OAS, verificou-se a necessidade de todos os processos referentes à tratamento de dados pessoais e requisitos da OEA exigidos serem cumpridos na integra pela organização.

Assim, um modelo de maturidade não se adequaria as necessidades do OAS Framework, visto que todos os módulos devem ser cumpridos de forma integral pelas empresas, não havendo brechas para um processo incompleto ou que não seja otimizado pela organização. Dessa forma, o objetivo específico “Elaborar níveis de maturidade do framework criado” acabou transformando-se em um modelo de implementação baseado no Ciclo PDCA, onde os módulos são dispostos de forma a auxiliar a organização adotante do OAS à uma adoção clara e concisa do framework. O desenvolvimento do modelo de implementação foi amplamente aprovado pelos especialistas entrevistados, mas ainda se faz necessária a aplicação fora do âmbito acadêmico para obter uma maior validação.

A realização da avaliação qualitativa do framework foi realizada com especialistas e os resultados expostos no capítulo 10 mostram uma ampla aprovação do OAS Framework, atendendo integralmente as necessidades das empresas que buscam adequação aos requisitos da certificação OEA e aderência com a LGPD. É importante ressaltar que apesar de aprovado pelos especialistas entrevistados, cabe em um futuro a análise de mais pessoas visando obter mais feedbacks sobre o artefato desenvolvido, possivelmente sendo aplicado em uma ou mais empresas buscando obter esse indicativo de aprovação.

O objetivo definido no Anteprojeto de realizar avaliação dos requisitos dos processos dos intervenientes de comércio exterior foi suprimida, visto o foco necessário dado aos processos de segurança de informação, que devem ser realizados de forma plena na busca da obtenção da certificação OEA.

A ideia do trabalho, deriva da já mencionada ausência de publicações relacionadas à certificação OEA e LGPD, no âmbito da implementação dos requisitos da certificação e dos artigos dispostos na legislação, assim, o trabalho desenvolvido será divulgado na intenção de ajudar a preencher essa lacuna acadêmica hoje existente.

É importante ressaltar também a importância de realizar em um futuro a aplicação do framework em organizações que enfrentem os desafios expostos no trabalho, assim havendo maior validação sobre o artefato proposto.

É notório que atualmente as ferramentas tecnológicas se desenvolvem de maneira exponencial, com várias novas tecnologias sendo criadas a todo momento. Assim, deve-se destacar que os controles que hoje atendem as necessidades das organizações podem ficar obsoletos após certos períodos, dessa forma, recomenda-se que sejam monitoradas regularmente as ferramentas e boas práticas comerciais no que tange a segurança da informação, esse não é um framework imutável e pode ser atualizado conforme a necessidade devida.

Dado o exposto acima, conclui-se que o Framework possui potencial, como indicado pela avaliação dos especialistas e possui espaço para auxiliar as organizações em seus processos de segurança da informação, contribuindo para o crescimento do comércio exterior brasileiro e proteção dos dados pessoais da população.

REFERÊNCIAS

Associação Brasileira de Normas Técnicas (ABNT). **NBR ISO/IEC 27001** – Tecnologia da informação – Técnicas de segurança – Sistemas de Gestão da Segurança - Requisitos. Rio de Janeiro: ABNT, 2013.

Associação Brasileira de Normas Técnicas (ABNT). **NBR ISO/IEC 27002** – Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013.

Associação Brasileira de Normas Técnicas (ABNT). **NBR ISO/IEC 27701** – Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro: ABNT, 2019.

AGRA, Andressa Dellay; BARBOZA, Fabrício Felipe Meleto. **Segurança de sistemas da informação**. [*S. l.: s. n.*], 2018. Disponível em: <https://integrada.minhabiblioteca.com.br/books/9788595027084>. Acesso em: 16 mar.

2021.ALENCAR, Gliner Dias; DE MOURA, Hermano Perrelli; JUNIOR, Alcides Jeronimo de Almeida information security policy: a simplified model based on ISO 27002. **14th International Conference on Information Systems & Technology Management,** [*s. l.*], 2017.

BATISTA, Luana Scandian; OBREGÓN, Marcelo Fernando Quiroga. Os impactos do Regulamento Europeu Geral sobre Proteção de Dados (EU GDPR) no Brasil. **Derecho y Cambio Social.** [*s. l.*], 2020. Disponível em: <https://www.derechoycambiosocial.com/revista062/Los_impactos_del_Reglamento_Europeo.pdf >. Acesso em: 18 mai. 2021.

BRASIL. **Instrução Normativa RFB nº 1985, de 09 de Outubro de 2015.** Dispõe sobre o Programa Brasileiro de Operador Econômico Autorizado. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 2015.

BRASIL. **Lei nº 13709, de 14 de Agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 2018.

BRASIL. Ministério da Defesa. **Lei Geral de Proteção de Dados - LGPD.** Disponível em: <https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd >. Acesso em: 20 mar. 2021.

BRASIL. Receita Federal do Brasil. **Perguntas & Respostas – Programa Brasileiro**

de OEA. Disponível em: <www.receita.economia.gov.br/orientacao/aduaneira/importacao-e-exportacao/oea/espaco-do-operador-oea/biblioteca-do-oea/apresentacoes-oea/perguntas-respostas.pdf>. Acesso em: 10 mar. 2021.

BRASIL. Secretaria de Governo Digital. **Programa de Governança em Privacidade.** Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/OficinaPGP.pdf > Acesso em: 15 mai. 2021.

COSTA, Elaine. Estatísticas do Programa OEA. **Receita Federal**, 2021. Disponível em: < https://www.gov.br/receitafederal/pt-br/assuntos/aduana-e-comercio-exterior/importacao-e-exportacao/oea/estatisticas-do-programa-oea> Acesso em: 10 mai. 2021.

DA ROCHA, Camila Pereira *et al.* Segurança da Informação: A ISO 27.001 como Ferramenta de Controle para LGPD. **Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará**, [*s. l.*], v. 2, n. 3, p. 78–97, 2019.

DE ANDRADE, Alex Gois; CASSANO, Francisco Américo; DE SOUZA, Mariana Nicodemo. EFEITOS DA IMPLEMENTAÇÃO DO PROGRAMA OEA SOBRE EMPRESAS INTERESADAS NA CERTIFICAÇÃO VISANDO VANTAGEM COMPETITIVA. **Revista da FAE**, [*s. l.*], v. 21, n. 2, p. 95–116, 2018.

FERREIRA, Alexandre José Henriques. **Implementação de um Sistema de Gestão de Segurança da Informação em Conformidade com a ISO/IEC 27001**. 2020. 63 f. Relatório de estágio (Mestrado em Gestão) - Faculdade de Economia da Universidade de Coimbra, Coimbra, Portugal, 2020.

GARCIA, Kleber Samuel. **Adequabilidade para a certificação como operador econômico autorizado (OEA)**: aplicação em uma importadora do estado de Santa Catarina. 2012. 55 f. Trabalho de Conclusão de Curso (Monografia) - Curso de Ciências Contábeis, Universidade Federal de Santa Catarina, [*s. l.*], 2018.

GORDHAN, Pravin. Customs in the 21st Century. **World Customs Journal**, [*s. l.*], v. 1, n. 1, p. 49–54, 2007. Disponível em: <https://worldcustomsjournal.org/Archives/Volume%201,%20Number%201%20(Mar%202007)/00%20Complete%20Issue%20WCJ_Volume_1_Number_1.pdf#page=57 >. Acesso em: 02 mai. 2021.

HINTZBERGEN, J. *et al.* **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. [*S. l.*]: BRASPORT, 2018. Disponível em: <https://plataforma.bvirtual.com.br/Leitor/Publicacao/160044/epub/0>. Acesso em: 14 mar.

2021.

IRAMINA, Aline. RGPD V. LGPD: Adoção Estratégica da abordagem responsiva na elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento geral de proteção de dados da União Europeia. **Revista de Direito, Estado e Telecomunicações**, [*s. l.*], v. 12, n. 2, 2020.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA). **COBIT 5** - Modelo Corporativo para Governança e Gestão de TI da Organização. ISACA, 2012.

ISO/IEC. International Standard. **ISO/IEC 27000** - Information technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary. ISO/IEC, 2018.

JAPPUR, Rafael Feyh. **Modelo conceitual para criação, aplicação e avaliação de jogos educativos digitais**. 2014. 296 f. Tese (Doutorado em Engenharia e Gestão do Conhecimento) - Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento, Universidade Federal de Santa Catarina, [*s. l.*], 2014.

JÚNIOR, Severino Domingos da Silva; COSTA, Francisco José. Mensuração e escalas de verificação: uma análise comparativa das escalas de Likert e Phrase Completion. **PMKT--Revista Brasileira de Pesquisas de Marketing, Opinião e Mídia**, [*s. l.*], v. 15, n. 1–16, p. 61, 2014.

LORENZON, Laila Neves. ANÁLISE COMPARADA ENTRE REGULAMENTAÇÕES DE DADOS PESSOAIS NO BRASIL E NA UNIÃO EUROPEIA (LGPD E GDPR) E SEUS RESPECTIVOS INSTRUMENTOS DE ENFORCEMENT. **Revista do Programa de Direito da União Europeia**, [*s. l.*], v. 1, p. 39–52, 2021.

MACHADO, Luiz Henrique Travassos *et al.* A facilitação comercial e o Programa Brasileiro de Operador Econômico Autorizado (OEA): histórico e lacunas. **Caderno de Finanças Públicas**, [*s. l.*], n. 15, p. 5–31, 2015.

MAGALHÃES, Pedro M. Requisitos e recomendações para o desenvolvimento e operação de um SGSI - Abordagem com ISO 27001/27002. **Cibersegurança e Informática Forense, Instituto Politécnico de Leiria.** [*s. l.*], jan. 2021. Disponível em: <https://www.researchgate.net/publication/348663585_Requisitos_e_recomendacoes_para_o_desenvolvimento_e_operacao_de_um_SGSI_-_Abordagem_com_ISO_2700127002>. Acesso em: 20 mai 2021.

PACHECO, Ana Paula Reusing *et al.* O ciclo PDCA na gestão do conhecimento: uma abordagem sistêmica. **Universidade Federal de Santa Catarina--Programa de Pós-**

Graduação em Engenharia e Gestão do Conhecimento [Internet], [*s. l.*], 2012.

PARANHOS, Maurício Machado. **Framework de segurança da informação para medição do nível de maturidade das organizações**. 2010. 239 f. Dissertação (Mestrado em Gestão do Conhecimento e da Tecnologia da Informação) - Universidade Católica de Brasília, Brasília, DF, 2010.

PEFFERS, Ken *et al.* A design science research methodology for information systems research. **Journal of management information systems**, [*s. l.*], v. 24, n. 3, p. 45–77, 2007.

PEREIRA, Cristiano; FERREIRA, Carlos. Identificação de Práticas e Recursos de Gestão do Valor das TI no COBIT 5. **RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação**, [*s. l.*], v. 15, n. 6, p. 17–33, 2015.

PEREIRA II, Celso Alves *et al.* Como Aproveitar Oportunidades Como Operador Econômico Autorizado da Receita Federal. **Revista IPTEC**, [*s. l.*], v. 6, n. 1, p. 1–18, 2018.

PEREIRA, Nayara Baccan; MORINI, Cristiano; GREGORACCI, Letícia Bueno. O Programa Operador Econômico Autorizado (OEA) no Comércio Internacional: Uma análise qualitativa a partir de sua implementação. **XVII SemeAD - Seminários em Administração**, [*s. l.*], out. 2014.

RAZUMEY, M. Role of the authorized economic operators in providing the state foreign trade safety. **Academy of Customs Service of Ukraine**, [*s. l.*], 2014.

RICARDO R., Mendes *et al.* Uma metodologia para implantação de um Sistema de Gestão de Segurança da Informação (SGSI) baseado nas normas ABNT NBR ISO/IEC 27001 e 27002. **Revista Principia**, [*s. l.*], v. 1, n. 22, p. 69–80, 2015. Disponível em: <https://search.ebscohost.com/login.aspx?direct=true&db=edsdoj&AN=edsdoj.862a52b323f74fc48a23bdddd01339a5&lang=pt-br&site=eds-live&scope=site>. Acesso em: 20 mai. 2021.

RIOS, Orlivaldo Kleber Lima; TEIXEIRA FILHO, José Gilson de Almeida; DA SILVA RIOS, Vânia Patrícia. Melhores práticas do COBIT, ITIL e ISO/IEC 27002 para implantação de política de segurança da informação em Instituições Federais do Ensino Superior. **Revista Gestão & Tecnologia**, [*s. l.*], v. 17, n. 1, p. 130–153, 2017.

SANTOS, Diana Leite Nunes Dos. **Avaliação da capacidade dos processos de governança corporativa de TI baseada no COBIT 5**. 61 f. Dissertação (Mestrado em Gestão do Conhecimento e da Tecnologia da Informação) - Universidade Católica de Brasília, Brasília, DF, 2013.

SILVA JUNIOR, Walter Thomaz da. **Programa do operador econômico autorizado brasileiro: uma oportunidade de negócios.** 2019. 59 f. Dissertação (Mestrado Profissional em Administração do Desenvolvimento de Negócios) - Universidade Presbiteriana Mackenzie

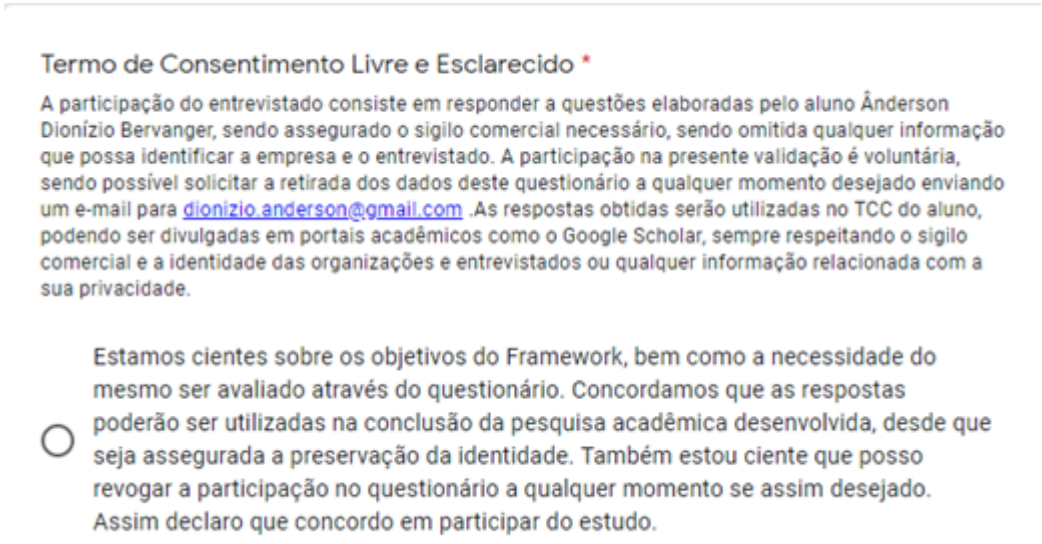
[*s. l.*], 2019.

TWEDDLE, Doug. Logistics, security, and compliance: The part to be played by authorized economic operators (AEOs) and data management. **World Customs Journal**, [*s. l.*], v. 2, n. 1, p. 101–105, 2008. Disponível em: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.739.158&rep=rep1&type=pdf#page=107>. Acesso em: 03 mai. 2021.

VIEIRA, Victor Rodrigues Nascimento. **Lei Geral de Proteção de Dados: Uma análise da tutela dos dados pessoais em casos de transferência internacional.** 2019. 77 f. Trabalho de Conclusão de Curso (Monografia) - Curso de Direito, Universidade Federal de Uberlândia, Uberlândia, MG, 2019.

APÊNDICE A – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

O termo de consentimento livre e esclarecido descreve o objetivo da pesquisa e esclarece o compromisso com a anonimização das informações comerciais envolvidas.



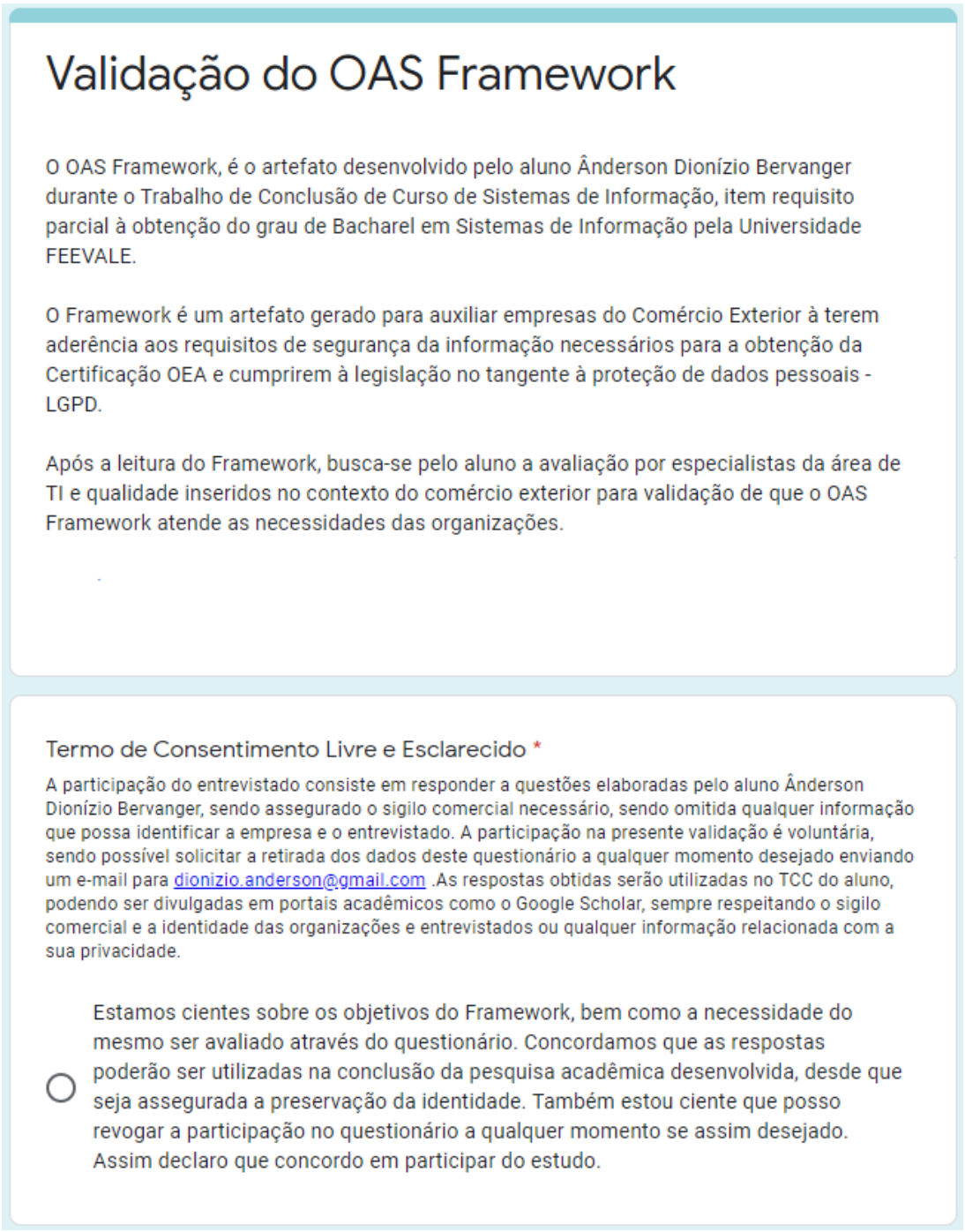
Termo de Consentimento Livre e Esclarecido *

A participação do entrevistado consiste em responder a questões elaboradas pelo aluno Ânderson Dionízio Bervanger, sendo assegurado o sigilo comercial necessário, sendo omitida qualquer informação que possa identificar a empresa e o entrevistado. A participação na presente validação é voluntária, sendo possível solicitar a retirada dos dados deste questionário a qualquer momento desejado enviando um e-mail para dionizio.anderson@gmail.com .As respostas obtidas serão utilizadas no TCC do aluno, podendo ser divulgadas em portais acadêmicos como o Google Scholar, sempre respeitando o sigilo comercial e a identidade das organizações e entrevistados ou qualquer informação relacionada com a sua privacidade.

○ Estamos cientes sobre os objetivos do Framework, bem como a necessidade do mesmo ser avaliado através do questionário. Concordamos que as respostas poderão ser utilizadas na conclusão da pesquisa acadêmica desenvolvida, desde que seja assegurada a preservação da identidade. Também estou ciente que posso revogar a participação no questionário a qualquer momento se assim desejado. Assim declaro que concordo em participar do estudo.

APÊNDICE B – QUESTIONÁRIO DE AVALIAÇÃO DO OAS FRAMEWORK

O Questionário de Avaliação do OAS Framework constitui-se de quinze (15) questões que foram elaboradas para entender a realidade do entrevistado e da empresa a qual ele representa e suas percepções sobre o Framework desenvolvido.



Validação do OAS Framework

O OAS Framework, é o artefato desenvolvido pelo aluno Ânderson Dionízio Bervanger durante o Trabalho de Conclusão de Curso de Sistemas de Informação, item requisito parcial à obtenção do grau de Bacharel em Sistemas de Informação pela Universidade FEEVALE.

O Framework é um artefato gerado para auxiliar empresas do Comércio Exterior à terem aderência aos requisitos de segurança da informação necessários para a obtenção da Certificação OEA e cumprirem à legislação no tangente à proteção de dados pessoais - LGPD.

Após a leitura do Framework, busca-se pelo aluno a avaliação por especialistas da área de TI e qualidade inseridos no contexto do comércio exterior para validação de que o OAS Framework atende as necessidades das organizações.

Termo de Consentimento Livre e Esclarecido *

A participação do entrevistado consiste em responder a questões elaboradas pelo aluno Ânderson Dionízio Bervanger, sendo assegurado o sigilo comercial necessário, sendo omitida qualquer informação que possa identificar a empresa e o entrevistado. A participação na presente validação é voluntária, sendo possível solicitar a retirada dos dados deste questionário a qualquer momento desejado enviando um e-mail para dionizio.anderson@gmail.com .As respostas obtidas serão utilizadas no TCC do aluno, podendo ser divulgadas em portais acadêmicos como o Google Scholar, sempre respeitando o sigilo comercial e a identidade das organizações e entrevistados ou qualquer informação relacionada com a sua privacidade.

○ Estamos cientes sobre os objetivos do Framework, bem como a necessidade do mesmo ser avaliado através do questionário. Concordamos que as respostas poderão ser utilizadas na conclusão da pesquisa acadêmica desenvolvida, desde que seja assegurada a preservação da identidade. Também estou ciente que posso revogar a participação no questionário a qualquer momento se assim desejado. Assim declaro que concordo em participar do estudo.

Nome e e-mail para contato *

Sua resposta

Avaliação sobre a empresa/entrevistado

Nesta seção, serão realizadas questões sobre a empresa do entrevistado

Dentro da organização, qual a posição que você ocupa atualmente? *

Sua resposta

Como você considera seu conhecimento a respeito da OEA e seus requisitos: *

	1	2	3	4	5	
Nenhum conhecimento	○	○	○	○	○	Bom conhecimento

Como você considera seu conhecimento a respeito da LGPD e seus requisitos: *

	1	2	3	4	5	
Nenhum conhecimento	○	○	○	○	○	Bom conhecimento

A empresa a qual você representa já possui a certificação OEA? *

Escolher

Avaliação sobre a empresa/entrevistado

Caso a resposta seja sim, quanto tempo faz que sua empresa é certificada como Operador Econômico Autorizado? *

- [ ] Mais de 5 anos
- [ ] De 5 anos à 3 anos
- [ ] De 3 anos à 1 ano
- [ ] Menos de 1 ano

Avaliação sobre a empresa/entrevistado

Caso a resposta seja não, em que status ela melhor se enquadraria em relação à OEA: *

- [ ] Estamos avaliando as vantagens e desvantagens
- [ ] Estamos decididos à obter a certificação, mas ainda não começamos os esforços
- [ ] Começamos os estudos e esforços para obter a certificação
- [ ] Estamos aguardando a avaliação pela Receita Federal
- [ ] Outro: _____

Avaliação sobre a empresa/entrevistado

Em relação à LGPD, como você avalia a aderência da sua organização em relação a legislação: *

- [ ] Não aderente
- [ ] Em processo de adequação
- [ ] Totalmente aderente

Avaliação sobre o OAS Framework

Em relação aos requisitos de segurança da informação dispostos pela OEA, o framework atende integralmente aos requisitos propostos: *

	1	2	3	4	5	
Discordo Totalmente	○	○	○	○	○	Concordo Totalmente

Em relação aos artigos dispostos na LGPD, os controles propostos pelo Framework facilitam a adequação das organizações ao que é exigido pela legislação: *

	1	2	3	4	5	
Discordo Totalmente	○	○	○	○	○	Concordo Totalmente

Os módulos do framework estão dispostos de maneira clara e eficiente, de forma a facilitar a utilização do OAS nas organizações *

	1	2	3	4	5	
Discordo Totalmente	○	○	○	○	○	Concordo Totalmente

O OAS cumpre sua proposta de ser um framework que organizações podem utilizar para se adequar aos critérios de elegibilidade da gestão da informação que compreendem aos requisitos de segurança da informação para obter a certificação OEA e que buscam estar de acordo com a LGPD: *

	1	2	3	4	5	
Discordo Totalmente	○	○	○	○	○	Concordo Totalmente

Os controles propostos contribuem para melhorar a segurança da informação na organização: *

	1	2	3	4	5	
Discordo Totalmente	○	○	○	○	○	Concordo Totalmente

O modelo de implementação do framework proposto é de fácil compreensão e facilita a sua aplicação: *

	1	2	3	4	5	
Discordo Totalmente	○	○	○	○	○	Concordo Totalmente

O OAS Framework é capaz de apoiar o processo de adequação aos requisitos da OEA e LGPD: *

	1	2	3	4	5	
Discordo Totalmente	○	○	○	○	○	Concordo Totalmente

Sugestões e críticas sobre o Framework: *

O que pode melhorar? O que não ficou claro ou que não se adequa a realidade da organização?

Sua resposta