LUIZ AUGUSTO FONSECA MONFARDINI

ANÁLISE DAS MEDIDAS DE PROTEÇÃO DAS INFORMAÇÕES ECONÔMICO-FISCAIS NO SERPRO ACERCA DA ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA

Trabalho de Conclusão de Curso - artigo científico - apresentado à Comissão de Avaliação de TCC da Escola Superior de Guerra - Campus Brasília, como exigência parcial para obtenção do título de Especialista em Altos Estudos em Defesa.

Orientador: Cel. Cláudio Alfredo Cunha Dornelles

Brasília
2020

LUIZ AUGUSTO FONSECA MONFARDINI (101186450)
Autor

LUIZ AUGUSTO FONSECA MONFARDINI

ANÁLISE DAS MEDIDAS DE PROTEÇÃO DAS INFORMAÇÕES ECONÔMICO-FISCAIS NO SERPRO ACERCA DA ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA

Trabalho de Conclusão de Curso apresentado à Escola Superior de Guerra – Campus Brasília, como exigência parcial para a obtenção do título de Especialista em Altos Estudos em Defesa.

Trabalho de Conclusão de Curso **APROVADO**:

Brasília, DF, 22 de Outubro de 2020

CLÁUDIO ALFREDO CUNHA DORNELLES (Cel R1 EB)
Orientador

THADEU LUIZ CRESPO ALVES NEGRÃO (Cel R1 EB)
Avaliador 1

Profa. Dra. CINTIENE SANDES MONFREDO MENDES (ESG/RJ)
Avaliador 2

Análise das medidas de proteção das informações econômico-fiscais no SERPRO acerca da Estratégia Nacional de Segurança Cibernética.

Luiz Augusto Fonseca Monfardini[1]

RESUMO

Em um mundo cada vez mais conectado, informações econômico-fiscais são muito sensíveis, inclusive as relacionadas com as altas autoridades dos três poderes da República. Estas informações são estratégicas e de grande relevância para a Segurança e Defesa do País. Este artigo objetiva analisar as medidas e os mecanismos de proteção das informações econômico-fiscais federais do Brasil no Serviço Federal de Processamento de Dados (SERPRO) verificando sua aderência com a Estratégia Nacional de Segurança Cibernética aprovada recentemente pelo Decreto nº 10.222, de 5 de fevereiro de 2020 e descrever potenciais riscos estratégicos ligados as áreas de Segurança e Defesa. A pesquisa é justificada na medida em que, aprimorando-se os mecanismos de proteção das informações econômico-fiscais, aumentar-se-á a sua proteção e disponibilidade, além de sua confiabilidade. A pesquisa realizada foi qualitativa de caráter exploratório. Como resultado, conclui-se que a estrutura interna de gestão de segurança da informação e governança cibernética e os projetos e ações da empresa estão alinhados à estratégia E-Ciber, na busca do permanente aumento da segurança dos sistemas e dados dos brasileiros.
Palavras-chave: Segurança da Informação. Estratégia Nacional de Segurança Cibernética. Serviço Federal de Processamento de Dados. Desafios e Lições Aprendidas.

Analysis of measures to protect economic and tax information in the Federal Data Processing Service (SERPRO) about the National Cybersecurity Strategy.

ABSTRACT

In an increasingly connected world, economic-fiscal information is very sensitive, including that related to the high authorities of the Republic. This information is strategic and of great relevance for the Security and Defense of the Country. This article aims to analyze the measures and mechanisms for protecting the federal economic-fiscal information of Brazil in the Federal Data Processing Service (SERPRO), verifying its adherence with the National Cybersecurity Strategy recently approved by Decree nº 10.222, of February 5, 2020 and describe potential strategic risks related to the areas of Security and Defense. The research is justified as, by improving the mechanisms for protecting economic-fiscal information, its protection and availability will be increased and its reliability. The research carried out was qualitative with an exploratory character. As a result, it is concluded that the internal structure of information security management and cyber governance and the company's projects and actions are aligned with the E-Ciber strategy, in the quest to increase the security of Brazilians' systems and data.
Keywords: *Information security. National Cybersecurity Strategy. Federal Data Processing Service. Challenges and Lessons Learned.*

[1] Auditor-Fiscal da Receita Federal do Brasil. Trabalho de Conclusão do Curso de Altos Estudos em Defesa da Escola Superior de Guerra, Campus Brasília, 2020.

1. INTRODUÇÃO

O SERPRO é uma empresa pública de prestação de serviços em tecnologia da informação do Brasil, e foi criado pela Lei nº 4.516, de 1 de dezembro de 1964, sendo vinculado ao Ministério da Economia, desenvolve sistemas e serviços que permitem controle e transparência sobre a receita e os gastos públicos.

Em um mundo cada vez mais conectado, informações econômico-fiscais são muito sensíveis, inclusive as relacionadas com as altas autoridades dos três poderes da República. Estas informações são estratégicas e de grande relevância para a Segurança e Defesa do País.

Atualmente, diversos sistemas e informações econômico-fiscais geridas pela Receita Federal do Brasil e pelo Ministério da Economia, tais como Imposto de Renda de Pessoas Física (IRPF), Portal Único do Comércio Exterior, Cadastro de Pessoas Físicas (CPF), Cadastro Nacional de Pessoas Jurídicas (CNPJ), Sistema Público de Escrituração Digital (SPED), dentre outros, são desenvolvidos e hospedados pelo Serviço Federal de Processamento de Dados (SERPRO).

O tema deste trabalho está relacionado com a verificação da aderência das medidas e dos mecanismos de proteção das informações econômico-fiscais federais do Brasil no SERPRO com a Estratégia Nacional de Segurança Cibernética (E-Ciber) aprovada recentemente pelo Decreto nº 10.222, de 5 de fevereiro de 2020, e descrever potenciais riscos estratégicos ligados à Defesa do Brasil.

A proteção das informações no SERPRO é um assunto relevante para a E-Ciber, que é uma orientação manifesta do Governo Federal à sociedade brasileira acerca das principais ações por ele pretendidas, em âmbito nacional e internacional, na área de segurança cibernética, tendo validade para o quadriênio 2020-2023, justificando este tema como de extrema importância para a Defesa Nacional.

A E-Ciber, além de ser o arcabouço normativo nacional sobre segurança cibernética, estabeleceu ações para modificar, de forma cooperativa e em âmbito nacional, características que refletem o posicionamento do Brasil sobre o assunto (BRASIL, 2020).

Ainda em decorrência da E-Ciber, foi recomendado que cada órgão do setor público e do setor privado planeje e realize gestões no sentido de colocar em prática os aspectos que lhe cabem e que devem ser estabelecidos nas suas ações estratégicas, em prol do pleno alcance dos objetivos estratégicos do Brasil no tema da segurança cibernética nacional.

Assim, a E-Ciber traz para o Brasil a visão de tornar-se um país de excelência em segurança cibernética, estabelecendo os seguintes objetivos estratégicos:

a) Tornar o Brasil mais próspero e confiável no ambiente digital;
b) Aumentar a resiliência brasileira às ameaças cibernéticas; e
c) Fortalecer a atuação brasileira em segurança cibernética no cenário internacional.

Diante do quadro apresentado, a questão relacionada ao problema deste artigo é o seguinte: como o SERPRO implementa as principais ações da E-Ciber relacionadas a sua atividade finalística?

A hipótese levantada é de que as informações gerenciadas pelo SERPRO devem estar bastante aderentes à estratégia E-Ciber, dada a criticidade na proteção das informações econômico-fiscais federais dos cidadãos e das empresas brasileiras, pois são de extrema importância para a área de Defesa, visando ainda mitigar eventuais riscos à segurança destas informações geridas pelo Estado Brasileiro.

Este trabalho objetiva analisar as ações estratégicas propostas na E-Ciber relacionadas às atividades do SERPRO, comparando-as com as ações implementadas pela empresa nos diversos sistemas de informação governamentais desenvolvidos e hospedados, verificando sua aderência a esta estratégia, de modo a mitigar eventuais riscos à área de Defesa e Segurança das Informações do Estado Brasileiro e de seus cidadãos.

Em relação aos objetivos específicos, o presente trabalho busca identificar no SERPRO as atividades relacionadas às ações estratégicas definidas na E-Ciber, com destaque para as seguintes:

a) Identificar as ações de governança cibernéticas no SERPRO;
b) Identificar o nível de maturidade em segurança cibernética do SERPRO;
c) Identificar as ações para elevar o nível de proteção dos dados no SERPRO;
d) Identificar a concepção de soluções inovadoras em segurança cibernética no SERPRO.

A pesquisa é justificada na medida em que, aprimorando-se os mecanismos de proteção das informações econômico-fiscais, aumentar-se-á a sua proteção e disponibilidade e, consequentemente, sua confiabilidade.

Decidiu-se adotar o método de pesquisa qualitativa, de caráter exploratório (pesquisa explorativa), por ser considerado o mais apropriado para este tipo de análise que se pretende

realizar. Assim, contextualizando este tipo de pesquisa escolhido, para o melhor entendimento do assunto, considera-se que esta pesquisa "é realizada em áreas na qual há pouco conhecimento acumulado e sistematizado. Por sua natureza de sondagem, não comporta hipóteses que, todavia, poderão surgir durante ou ao final da pesquisa" (VERGARA, 2009, p. 42).

Ademais, nesta pesquisa qualitativa de caráter exploratório, utilizou-se a pesquisa de campo com pessoas que participam desse processo de gestão de segurança da informação na empresa, além de fontes de dados documentais e análises de dados, documentos e relatórios fornecidos pelo SERPRO.

Em relação a estes meios de investigação, utilizou-se a pesquisa de campo porque também de acordo com Vergara, é: "investigação empírica realizada no local onde ocorre ou ocorreu um fenômeno ou que dispõe de elementos para explicá-lo. Pode incluir entrevistas, aplicação de questionários, testes e observação participante ou não" (VERGARA, 2009, p. 43).

Visando a sua fundamentação, esta pesquisa parte também do Decreto nº 10.222, de 5 de fevereiro de 2020, sobretudo no que se refere a algumas atividades relacionadas às ações estratégicas definidas no mesmo para órgãos públicos (BRASIL, 2020).

Na revisão da literatura sobre o tema, inicialmente, em cada seção, far-se-á menção à literatura e/ou aos documentos de governança cibernética que discorrem sobre a implementação e manutenção de cada ação. Posteriormente, são elencadas as principais atividades da E-Ciber relacionadas à governança de segurança da informação no SERPRO.

No decorrer do trabalho, serão analisados apresentados referenciais teóricos de cada atividade, que tenham relação com o tema proposto, bem como alguns trabalhos de pesquisadores que estudaram a área de segurança da informação e governança cibernética.

Assim, na próxima seção serão abordadas as ações de governança cibernética no SERPRO. Em seguida, são apresentados insumos sobre o nível de maturidade em governança cibernética da empresa. Na quarta seção deste trabalho, são apresentadas as ações para elevar o nível de proteção de seus dados. Após, a concepção de soluções inovadoras em segurança cibernética no SERPRO e, por fim, as considerações finais do presente trabalho.

2. AÇÕES DE GOVERNANÇA CIBERNÉTICA NO SERPRO

Dentre as diversas iniciativas para articulação e normatização de temas relacionados à politica de segurança cibernética, pode-se citar o Marco Civil da Internet (BRASIL, 2014) e a Lei Geral de Proteção de Dados Pessoais – LGPD (BRASIL, 2018b) que, juntamente com o Decreto da E-Ciber (BRASIL, 2020), formam um arcabouço normativo de governança cibernética e, consequentemente, de segurança da informação.

Acerca da grande abrangência da área de segurança da informação, a E-Ciber definiu que: "a Estratégia Nacional de Segurança da Informação seja construída em módulos, a fim de contemplar a segurança cibernética, a defesa cibernética, a segurança das infraestruturas críticas, a segurança da informação sigilosa e a proteção contra vazamento de dados" (BRASIL, 2020).

A E-Ciber estabeleceu como ação de governança estratégica o fortalecimento das ações de governança em segurança cibernética, por parte do setor público e do setor privado, contemplando iniciativas relacionadas à gestão de pessoas, ao atendimento aos requisitos de segurança cibernética e à gestão dos ativos de informação. A E-Ciber traz ainda exemplos de ações que podem ser realizadas neste sentido, como a criação de comitês e fóruns de governança, com a definição de requisitos mínimos de segurança cibernética nas contratações, programas e projetos sobre governança cibernética, a ampliação do uso do certificado digital, a adoção de padrões internacionais no desenvolvimento de novos produtos, dentre outros.

Acerca do tema de políticas de minimização dos riscos e do aumento no nível de segurança das informações, Correia (2017) apresenta um trabalho com uma análise de mais de trinta comitês de tecnologia da informação. Nestes casos, é comum ser parte das atribuições destes comitês executivos de tecnologia da informação as atividades relacionadas à gestão da segurança da informação, sendo este modelo encontrado em muitos órgãos da administração pública federal.

Seguindo boas práticas internacionais, e conforme estabeleceu o Decreto nº 9.203, de 22 de novembro de 2017, "compete à alta administração dos órgãos implementar e manter mecanismos, instâncias e práticas de governança" (BRASIL, 2017).

Assim, acerca das ações de governança em segurança da informação e governança cibernética relacionada a E-Ciber no SERPRO, em 31 de agosto de 2004, foi criado o Comitê Permanente de Segurança da Informação (CPSI), e o estabelecimento do Programa de

Segurança do SERPRO (PSS) através da decisão de diretoria 73/2004, assinada pelo então diretor-presidente da empresa. O referido comitê foi alterado posteriormente pela empresa em 2008, 2011, 2016, 2018 e, recentemente em 2019, onde foi apresentada ata de reunião do agora denominado Comitê Estratégico de Governança, Riscos, Controles e Segurança da Informação - COGRS, que reforça o objetivo do comitê de atuar em nível estratégico, sobre a condução das políticas, regras e práticas de governança corporativa, gestão de riscos, controles internos, segurança da informação, gestão de continuidade do negócio no SERPRO e governança de dados, mantendo seu alinhamento à estratégia empresarial.

Este comitê atualmente é composto pelos seguintes membros:

a) Coordenador Titular sendo o Diretor Jurídico e de Governança e Gestão – DIJUG;

b) Coordenador Substituto sendo o Diretor de Operações – DIOPE;

c) Superintendente de Gestão Financeira – SUPGF;

d) Superintendente de Controladoria – SUPCO;

e) Superintendente de Controle, Riscos e Conformidade – SUPCR;

f) Superintendente de Segurança da Informação – SUPSI;

g) Superintendente de Produtos e Serviços – Operações – SUPOP;

h) Superintendente de Soluções Analíticas e Inteligência Artificial – SUPAI;

i) Superintendente de Serviços de Engenharia de Solução Digital – SUPSE;

j) Superintendente de Estratégia Comercial – SUNEC;

k) Coordenação de Suporte Administrativo DIRCL – COADM;

l) Superintendente de Gestão de Pessoas – SUPGP; e

m) Superintendente de Educação – SUPED.

Ademais, este comitê (COGRS) é o órgão colegiado de pronúncia, atualização e proteção às seguintes políticas:

a) Política Corporativa de Gestão de Riscos, Controles e Conformidade -

PCGRC;

b) Política Corporativa de Segurança da Informação do SERPRO – PCSI;

c) Política Corporativa de Continuidade do Negócio – PCCN; e

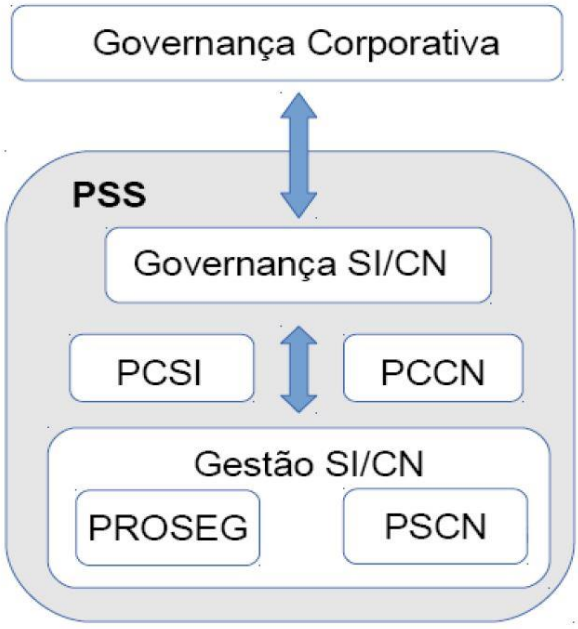
d) Política Corporativa de Governança de Dados – PCGD.

Verifica-se que estas quatro políticas estão em vigor e, sendo permanentemente atualizadas, fornecem um sólido arcabouço normativo em segurança cibernética para a

empresa e seus produtos e serviços.

Além destas políticas, foi apresentado também o Programa de Segurança do SERPRO - PSS que contempla os modelos de governança e de gestão da segurança da informação e de continuidade de negócios, atendendo às orientações das Políticas Corporativas de Segurança da Informação (PCSI) e de Continuidade de Negócios (PCCN). O PSS é descrito como tendo um ciclo de vida contínuo e de âmbito corporativo. Desta forma, estas políticas orientam na definição e adoção dos normativos para o SERPRO e em suas unidades organizacionais, de forma a gerenciar riscos e garantir a recuperação em caso de indisponibilidade por eventos significativos. A figura 1 apresenta a relação entre a Governança Corporativa, o PSS e as demais políticas descritas.

Figura 1 – Diagrama representando a relação entre a Governança Corporativa, o Programa de Segurança do SERPRO e das demais políticas corporativas.



Fonte: SERPRO (2019c)

O PSS do SERPRO, conforme suas diretrizes, objetiva manter o alinhamento entre as ações de governança e de gestão da Segurança da Informação e Continuidade de Negócios (SI/CN) para assegurar o negócio da empresa nos aspectos de integridade, disponibilidade e confidencialidade da informação, visando:

- Apoiar o gerenciamento dos riscos de segurança da informação;
- Sistematizar as iniciativas de SI/CN;

• Orientar os gestores de SI/CN;

• Fomentar a cultura de SI/CN;

• Estabelecer e manter os normativos e os processos de SI/CN;

• Promover a melhoria contínua dos processos associados à SI/CN; e

• Garantir seu próprio alinhamento com a governança corporativa e com a governança de TI.

Desta forma, a empresa possui uma gestão permanente e contínua das políticas relacionadas à segurança da informação através da alta cúpula da empresa, gerindo as ações de governança cibernética perseguidas pela E-Ciber.

A seguir, serão abordadas algumas das principais avaliações acerca do nível de maturidade em governança cibernética do SERPRO.

3. NÍVEL DE MATURIDADE EM GOVERNANÇA CIBERNÉTICA DO SERPRO

Conforme Sêmola (2014) são muitos os que acreditam que o assunto de segurança da informação referem-se à aquisição de equipamentos e sistemas, especialmente os mais caros como, por exemplo, sistemas de proteção à intrusão, firewalls ou antivírus. Entendem que somente a implantação de políticas de defesa e a adoção de cuidados funcionais em relação à tecnologia são suficientes. Porém, deve-se ter em mente que nenhum desses dispositivos é capaz de prevenir perdas, se forem aplicados de forma solitária e imprudente.

Além disso, Roen (2017) descreve que a conscientização, educação e treinamento sobre segurança cibernética devem ser considerados como instrumentos de mudança organizacional e cultural, ampliando cada vez mais a integração das empresas e dos órgãos e, especialmente, entidades da Administração Pública Federal (APF), objetivando um processo contínuo de aprimoramento e evolução da segurança das informações dos governos, das empresas e dos cidadãos. Como forma a verificar o efetivo retorno de capacitação e implantação de soluções de segurança da informação, utilizam-se comumente os denominados modelos de maturidade em segurança da informação.

Estes modelos de maturidade são considerados uma técnica muito utilizada para análise comparativa de recursos na área de Tecnologia da Informação (TI). Lima (2017) propôs um modelo de maturidade composto por cinco níveis de maturidade, numerados em uma escala de 0 a 4. Cada nível é considerado um estágio evolutivo e tem um conjunto de metas de segurança

relacionadas à configuração de um dado componente de infraestrutura. Neste caso, é descrita uma escala numérica do nível de maturidade, onde são apresentados os níveis de maturidade, com uma nomenclatura de cada nível e o percentual de controles de segurança atendidos.

Estes degraus, ou níveis de maturidade, apresentam intervalos que são definidos por uma margem de porcentagem, de forma que seja possível produzir o índice. Esta forma também é comumente utilizada em diversos outros trabalhos, como Muthukrishnan e Palaniappan (2016).

Tabela 1 – Relação entre os níveis de maturidade e o percentual de controles atendidos.

Níveis de Maturidade	Nomenclatura	Controles Atendidos
0	Não Gerenciado (UM)	0-19,99 % dos controles
1	Inicialmente Gerenciado (IM)	20-39,99 % dos controles
2	Parcialmente Gerenciado (PM)	40-59,99 % dos controles
3	Largamente Gerenciado (WM)	60-79,99 % dos controles
4	Totalmente Gerenciado (FM)	80-100 % dos controles

Fonte: Lima (2017)

Acerca desse tema, a E-Ciber estabeleceu como ação de governança estratégica a elevação do nível de maturidade das empresas, além da sociedade, em segurança cibernética, com a finalidade de ampliar a compreensão dos riscos e das ameaças no espaço cibernético, de forma a possibilitar a todos um uso oportuno e adequado de procedimentos e de ferramentas a favor da utilização segura do ambiente digital (BRASIL, 2020).

A E-Ciber lista ainda alguns exemplos de iniciativas desta ação, tais como: conscientização da população, realização campanhas de conscientização interna em empresas e órgãos públicos, ampliação da capacitação de profissionais para atuar no combate aos crimes cibernéticos, promoção da gestão de conhecimento de segurança cibernética, dentre outras. Um excelente exemplo deste tipo de iniciativa, é a cartilha de segurança para a internet do Centro de Estudos para Resposta e Tratamento de Incidentes (CERT, 2020).

No caso do SERPRO, devido à criticidade do tema na gestão de dados econômico-fiscais, o desenvolvimento do programa gerador do imposto de renda IRPF criado em 1991, que possibilitou a entrega da declaração por meio magnético, e com a entrega da declaração de ajuste anual do imposto de renda em 1997 pela internet, fez-se necessário que a empresa desenvolvesse seus processos de gestão de segurança da informação neste período,

ou seja, desde a década de 90. Mais recentemente, no ano de 2013, com a possibilidade de entrega da declaração IRPF por dispositivos móveis, que formaram um novo universo tecnológico, estes processos de gestão de segurança da informação foram aprimorados. Assim, estes requisitos de segurança da informação, além desta cultura, sempre estiveram presentes na empresa, distribuídos em suas diversas áreas, além de seus produtos e serviços.

Mais recentemente, em 2019, com o objetivo de unificar esta gestão de segurança na empresa, foi criada uma área dedicada e única ao tema segurança da informação e segurança cibernética, integrando as áreas de infraestrutura, governança e produção de segurança da informação. Como resultado imediato, criou-se o Centro de Operações de Segurança (SOC), com o objetivo de impor uma atuação mais proativa, além de ampliar a monitoração da infraestrutura crítica, nos termos da Política Nacional de Segurança de Infraestruturas Críticas – PNSIC (BRASIL, 2018a).

Este SOC objetivou também a monitoração dos ataques direcionados aos sistemas estruturantes do governo brasileiro, além de ser responsável pela revisão dos processos e orientações de segurança para atender as determinações da governança corporativa e dos normativos federais.

Ainda como resultado da criação deste SOC, foi contratada em 2019 uma auditoria com a empresa Unisys, acerca de governança em segurança da informação.

A tabela 2 apresenta um dos resultados desta recente auditoria realizada pela empresa Unisys na estrutura de segurança da informação do SERPRO. Nesta auditoria, dentre outras, foram examinadas as eficácias dos controles de segurança da informação da empresa, acerca de diversas categorias de ameaças.

Tabela 2 - Pontuações de eficácia de controle (por categoria de ameaça)

	Threat Category								
Asset Group	WebApp Attack	Misuse	Error	Theft/Loss	Crimeware	Skimmers	Cyber Espionage	DoS Attack	Everything Else
Server/Apps	75%	73%	73%	71%	74%	70%	74%	85%	74%
Network	77%	75%	76%	77%	77%	76%	77%	85%	75%
End User Systems	73%	73%	72%	71%	74%	70%	73%	74%	74%
Critical IoT	75%	74%	73%	73%	74%	62%	74%	77%	75%
Media & Offline Data	70%	70%	70%	70%	70%		70%		70%
People	69%	72%	72%	70%	70%		70%	72%	72%

Fonte: SERPRO (2019d)

Pode-se verificar que, nesta análise, a menor pontuação na eficácia de controles foi 62% no item de *skimmers* (roubo de informações) em dispositivos críticos *IoT* (internet das coisas). Assim, ao comparar os percentuais de pontuação de eficácia de controles da auditoria (tabela 2) com a coluna de percentuais de controles atendidos nos níveis de maturidade (tabela 1) do trabalho de Lima (2017), que avalia justamente os percentuais de controles atendidos, verifica-se que o menor nível de percentual encontrado (62%) está no nível de maturidade 3, ou seja, Largamente Gerenciado (WM). Nesta comparação, pode-se verificar também que os controles estão, no geral, em um alto nível de maturidade, sendo inclusive alguns pontuados no nível 4 (Totalmente Gerenciado).

Em 2019, também foi criado o Escritório de Governança de Dados com os objetivos de: viabilizar a transformação digital do SERPRO, definir e adotar padrões, modelos, políticas, formação de cultura e boas práticas sobre o uso dos dados transacionais e analíticos, além de complementar outras ações voltadas à modernização da exploração de dados na empresa, como um novo banco de dados de governo (GovData), a criação de um centro de excelência em Inteligência Artificial (IA), assim como as ações educacionais da jornada de inteligência artificial.

A criação desse escritório vai ao encontro dos princípios preconizados pela LGPD, e pela E-Ciber, no que se referem à adoção das melhores práticas de governança, segurança da informação, gestão de riscos e conformidade.

A empresa também desenvolveu uma solução específica para a LGPD, que concentra todas as informações de titulares, encarregados, operadores e controladores de forma automática, demonstrando uma forte adesão à E-Ciber.

Na próxima seção serão apresentadas ações do SERPRO para elevar o nível de proteção dos dados armazenados na empresa, em especial o modelo NIST.

4. AÇÕES PARA ELEVAR O NÍVEL DE PROTEÇÃO DOS DADOS NO SERPRO

Diversas razões motivam os ataques cibernéticos. Dentre elas, pode-se citar o ataque a infraestruturas críticas e o uso de informações secretas como os principais motivos a terroristas atacarem governos. Em relação aos criminosos virtuais, destaca-se o roubo de propriedade intelectual ou dados financeiros como os principais motivadores. Neste sentido, a questão de atribuição de responsabilidade ainda é muito difícil (CRUZ JUNIOR, 2013).

Apesar disso, o Brasil já possui legislação específica sobre o assunto, através da Lei nº 12.737, de 30 de novembro de 2012, que especifica:

> "Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Pena - detenção [...]" (BRASIL, 2012).

De forma complementar, a E-Ciber estabeleceu como ação de governança estratégica a elevação do nível de proteção do governo, por intermédio de ações na área de segurança cibernética. A E-Ciber exemplificou as ações que podem ser adotadas neste sentido, tais como: o aperfeiçoamento do uso dos dispositivos de comunicação segura, a elaboração de requisitos específicos de segurança cibernética, a recomendação do uso de cópias de segurança atualizadas e segregadas de forma automática em local protegido e a manutenção da atualização dos sistemas informacionais, as infraestruturas e os sistemas de comunicação dos órgãos públicos, em relação aos requisitos de segurança cibernética (BRASIL, 2020).

No SERPRO, acerca destas ações para elevar o nível de proteção dos dados, a Superintendência de Segurança da Informação conduz oitenta e duas ações dentro de suas divisões. Estas ações foram distribuídas utilizando um *framework* de segurança cibernética (modelo NIST) que fornece uma estrutura, com base nos padrões, diretrizes e práticas existentes para organizações do setor privado nos Estados Unidos, a fim de gerenciar e reduzir melhor o risco de segurança cibernética. O modelo NIST permite que o SERPRO desenvolva sua base identificando o que precisa ser protegido, implantando proteções, detectando, respondendo e recuperando-se de eventos e incidentes. O modelo prevê as os seguintes aspectos: Identificar, Proteger, Detectar, Responder e Recuperar. Na figura a seguir é possível ver a distribuição destas funções, onde e como elas compõe o quadro de segurança cibernética do SERPRO.

Figura 2 – Distribuição das funções no modelo NIST

Fonte: SERPRO (2019b)

Acerca da distribuição das oitenta e duas ações do modelo, têm-se trinta e três ações na função identificar, vinte e duas ações na função proteger, nove ações na função detectar, doze ações na função responder e seis ações na função recuperar.

Dentre as trinta e três ações da empresa com a função de identificar, destacam-se algumas: a solução de inteligência preditiva de ataques, a análise de código-fonte como serviço, plataforma LGPD e a unificação de *login* nos equipamentos de segurança. Nas vinte e duas ações da empresa com a função de proteger, destacam-se: a implantação da nova solução de *firewalls*, a criação de um portal de automação de *firewall* e procedimentos a criação do de uma barreira para o governo. Nas nove ações da empresa com a função detectar, destacam-se: a análise de vulnerabilidade como serviço, e o teste de penetração em sistemas. Dentre as doze ações com a função de responder da empresa, podem-se destacar: o programa de gestão de vulnerabilidades, os ciclos de treinamentos em segurança da informação e a implantação e definição da forense computacional. Por fim, dentre as seis ações da empresa com a função de recuperar, destacam-se: o sistema de gestão de continuidade de negócios e a gestão de riscos em segurança da informação.

Com o intuito de garantir o elevado nível tecnológico e de governança cibernética da empresa, além de se manter em, no mínimo, nível de igualdade com outras empresas de vanguarda tecnológica, o SERPRO deu ênfase à atualização tecnológica de seus ambientes. A aquisição de novas soluções de segurança embasadas por estudos e prospecções e definidas de acordo com as melhores práticas de mercado, proporcionou à empresa mecanismos de atender

aos interesses do governo, além de garantir também o cumprimento dos seus objetivos institucionais. Tais esforços foram evidenciados em investimentos já realizados e em projeções de investimentos em segurança da informação, que para 2021 estão na ordem de R$26 milhões, somente em equipamentos de segurança da informação.

Como exemplo destes investimentos já realizados, destacam-se a aquisição de plataformas de segurança, objeto de estudo remodelado e de maior complexidade, onde se evidenciaram as seguintes ações e projetos: AlgoSec (solução de automação de *firewalls*), FCW (Filtro de Conteúdo *Web*), NIPS (*Network Intrusion Prevention System*) ou Sistema de Prevenção à Intrusão de Rede e *Firewalls* de representações regionais (atualização tecnológica). A seguir, detalha-se cada uma destas aquisições:

4.1. ALGOSEC (SOLUÇÃO DE AUTOMAÇÃO DE *FIREWALLS*)

Aquisição tecnológica necessária para proporcionar agilidade, automação e um mecanismo eficaz para auditorias, ampliando assim a base de clientes e, consequentemente, aumentando as vendas, onde o foco da solução foram os serviços de segurança oferecidos aos clientes, tanto em nuvem quanto em ambientes tecnológicos tradicionais. O principal benefício desta solução foi a redução da intervenção manual em equipamentos de segurança da informação, aumentando assim sua confiabilidade e a segurança. Outro benefício também obtido pela solução foi a diminuição dos custos dos serviços de segurança, pois foram reduzidas as necessidades de interação e gerenciamento destes equipamentos de segurança da informação, reduzindo assim o tempo para atendimento a demandas e novos projetos.

4.2. FCW (FILTRO DE CONTEÚDO *WEB*)

A atualização da solução de filtro de conteúdo foi necessária em razão do exponencial aumento da demanda de tráfego de Internet pelo governo federal e de conteúdos criptografado nos últimos anos, aumentando também o consumo de processamento nas redes do SERPRO, a ponto de impactar seus serviços e sistemas. Após a avaliação da aquisição, a solução foi totalmente redimensionada, considerando requisitos técnicos e de capacidade, resultando em um ambiente que atende as necessidades do governo, protegendo seu controle de acesso para os próximos anos.

4.3. NIPS (*NETWORK INTRUSION PREVENTION SYSTEM*)

A aquisição de uma solução deste tipo foi realizada na necessidade de complementar a proteção provida por outras tecnologias, fornecendo segurança em múltiplas camadas, atendendo a premissa de segurança focada em aplicações. Como a empresa já possuía experiência em plataformas desta natureza, após uma prospecção envolvendo os principais concorrentes do mercado, e de acordo com a consultoria em tecnologia Gartner Group, foi capaz de especificar uma solução altamente robusta e flexível, atendendo suas necessidades com um investimento relativamente reduzido, evitando assim a aquisição de capacidade e recursos desnecessários, mas obtendo tecnologia de ponta.

4.4. *FIREWALLS* DE REPRESENTAÇÕES REGIONAIS (ATUALIZAÇÃO TECNOLÓGICA)

A empresa optou por realizar uma atualização tecnológica de todas suas regionais, com vistas a atender os requisitos dos serviços atuais e do ambiente descentralizado do SERPRO. Esta opção considerou, dentre outros fatores, o *know-how* de mais de 20 anos das equipes técnicas na solução. A atualização tecnológica desta solução permitiu à empresa aumentar a sua capacidade instalada e o atendimento das demandas dos seus serviços em suas representações regionais, mesmo as que não possuem centros de dados, mas possuem necessidades em segurança da informação. Assim, com esta aquisição tecnológica, foi possível aperfeiçoar o parque de soluções de segurança da informação, consolidando fornecedores de diferentes soluções em um só, reduzindo riscos. Esta inovação permitiu a integração com tecnologias de automação de processos de segurança, garantindo assim um avanço no modelo de trabalho.

Observa-se que os investimentos em segurança da informação do SERPRO foram robustos, e priorizaram a adoção de medidas mais efetivas de proteção para maiores volumes de dados, além da mitigação no risco de prejuízos à imagem da empresa e do governo, e também maior confiabilidade às ações de perícia técnica em apoio a auditorias e sindicâncias, além de capacitação das equipes altamente especializadas na área de segurança da informação, atendendo ao estabelecido pela E-Ciber. Na próxima seção serão apresentadas as prospecções em soluções inovadoras em segurança cibernética em andamento no SERPRO.

5. CONCEPÇÃO DE SOLUÇÕES INOVADORAS EM SEGURANÇA CIBERNÉTICA NO SERPRO

Acerca do tema inovação, a E-Ciber (BRASIL, 2020) estabeleceu como ação de governança estratégica o incentivo à concepção de soluções inovadoras em segurança cibernética, de modo a incentivar a pesquisa e o desenvolvimento de soluções em segurança cibernética, trazendo a inovação aos produtos nacionais nessa área. Dentre as ações a serem consideradas, cita: a criação de centros de pesquisa e desenvolvimento em segurança cibernética no governo, a viabilização de investimentos na área, o desenvolvimento e a inovação de soluções de segurança cibernética nas tecnologias emergentes, a adoção de padrões globais de tecnologia, o incentivo ao desenvolvimento de solução em criptografia, além do estabelecimento de requisitos mínimos de segurança cibernética no uso de tecnologia de quinta geração de conexão móvel - 5G.

No SERPRO, além das seções anteriores, que já apresentaram soluções que podem ser enquadradas em algumas destas ações relacionadas na E-Ciber, estão sendo realizadas prospecções e desenvolvimento de outras soluções na área de segurança da informação, especialmente algumas provas de conceito (PoC), conforme a seguir:

5.1. PROSPECÇÃO DE SOLUÇÃO PARA ANONIMIZAÇÃO E CONTROLE DE ACESSO A INFORMAÇÃO PESSOAIS E PESSOAIS SENSÍVEIS EM CONFORMIDADE COM A LGPD (POC SOLUÇÃO *VORMETRIC DATA SECURITY*)

Esta prospecção objetiva a aplicação de controles, garantindo a anonimização dos dados e controle de acesso em conformidade com a LGPD (BRASIL, 2018b). A LGPD define como anonimização a “utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado pessoal perde a possibilidade de associação, direta ou indireta, com o seu titular” (BRASIL, 2018b). Esta prospecção tem com base a identificação de necessidades e oportunidades que se apresentam nos contextos atuais e futuros, derivados da obrigatoriedade de adequação de entidades públicas e privadas no que tange especialmente a proteção de dados pessoais.

A LGPD define requisitos mandatórios, que objetivam maior proteção das informações pessoais e sensíveis nos sistemas e bases de dados públicos e privados. Com a obrigatoriedade

de adequação à referida lei, bem como na sua função de servir o governo com o uso eficiente de soluções de tecnologia da informação, a empresa tem a missão de buscar inovações e ofertar serviços em seu portfólio de produtos que possam contribuir com o governo no tocante às adequações necessárias à LGPD.

5.2. PROSPECÇÃO DE SOLUÇÃO PARA MICRO-SEGMENTAÇÃO DE REDE PARA O CONTROLE DE TRÁFEGO HORIZONTAL (POC *STEALTH*)

A solução prospectada objetiva, através da micro-segmentação de segmentos de rede, uma camada adicional de segurança sobre a segmentação física da rede, com foco principal na proteção de tráfego de comunicação. Esta é uma tecnologia ainda muito recente e representa o estado da arte em segmentação de rede e proteção de infraestrutura.

5.3. PROSPECÇÃO DE SOLUÇÃO DO TIPO BAS (*BREACH AND ATTACK SIMULATION*) VISANDO A SIMULAÇÃO DE ATAQUES E DETECÇÃO DE VULNERABILIDADES NOS ATIVOS DE SEGURANÇA DE REDE (POC *PICUS*)

Esta prospecção tem como função principal a simulação de ataques e identificação de vulnerabilidades em ativos de redes. Com esta prospecção, o SERPRO busca meios de ampliar o seu portfólio de produtos com mais inovação para oferecer ao governo, identificando vulnerabilidades e demonstrando a necessidade de ampliação na segurança de rede, possibilitando correções e eliminação de vulnerabilidades.

5.4. PROSPECÇÃO DE EVOLUÇÃO NA SOLUÇÃO PARA AUTOMAÇÃO DE CONFIGURAÇÃO DE ROTEADORES E SWITCHES (POC *ALGOSEC*)

Com o objetivo de automatizar ainda mais processos ligados à infraestrutura, está sendo prospectada uma solução capaz de prover a automação da maior parte dos dispositivos de segurança e infraestrutura da empresa.

Uma maior integração entre segurança e infraestrutura de rede propicia um grande incremento nas camadas de proteção dos dados hospedados, além de redução de pessoal necessário para a manutenção dos ambientes, melhorando os índices de atendimento e

reduzindo riscos.

Desta forma, foram apresentadas quatro prospecções na área de segurança cibernética, demonstrando que a empresa permanece em constante atualização e aperfeiçoamento, em consonância ao estabelecido na E-Ciber.

A seguir são apresentadas as considerações finais do trabalho, onde é apresentado um resumo das ações que nortearam o presente estudo, com seus principais resultados e dificuldades, além de perspectiva de trabalhos futuros.

6. CONSIDERAÇÕES FINAIS

A Estratégia Nacional de Segurança Cibernética (E-Ciber), aprovada pelo Decreto 10.222, de 5 de fevereiro de 2020, foi elaborada com a meta de apresentar os direcionamentos que o governo federal considera essenciais para que o Brasil, e suas instituições, se tornem mais seguros e resilientes no uso do espaço cibernético. O presente trabalho apresentou um breve panorama das ações do Serviço Federal de Processamento de Dados (SERPRO) acerca da E-Ciber, avaliando os projetos e ações da empresa, e se estão alinhados à estratégia, na busca do aumento da segurança dos sistemas e dados armazenados por esta empresa pública.

No decorrer deste estudo, constatou-se que o SERPRO possui uma estrutura interna de gestão de segurança da informação e governança cibernética robusta, e que está alinhada aos propósitos da E-Ciber. Possui um conjunto de políticas internas, em especial: Política Corporativa de Gestão de Riscos, Controles e Conformidade (PCGRC), Política Corporativa de Segurança da Informação do SERPRO (PCSI), Política Corporativa de Continuidade do Negócio (PCCN) e Política Corporativa de Governança de Dados (PCGD), todas aprovadas por seu Comitê Estratégico de Governança, Riscos, Controles e Segurança da Informação. Além disso, apresentou um alto nível de maturidade na área de segurança da informação, conforme boas práticas de mercado, implementando modelos que são referência mundial, como o NIST, obtendo também altos percentuais de eficácia de controles até em auditoria externa. Ao final, foi apresentado um conjunto de ações e projetos voltados para a ampliação dos atuais níveis de governança em segurança cibernética, além de projetos potencialmente inovadores na busca pelas tecnologias mais modernas da área.

Dentre os desafios do presente estudo, pode-se mencionar a impossibilidade de visita presencial ao Centro de Operações de Segurança (SOC) da empresa, que traria maior imersão nos processos de gestão de segurança da informação e governança cibernética da empresa.

Esta visita está restrita no presente momento devido à situação atual mundial de pandemia. Além deste desafio, a restrição de divulgação de algumas informações de gestão da segurança cibernética da empresa também se apresentou como desafio, aumentando os cuidados com o acesso e divulgação de dados desta natureza, especialmente por ser uma empresa pública que atende principalmente ao governo federal.

Um aspecto organizacional a ser ressaltado foi a excelente disponibilidade dos entrevistados, gestores de alto nível da Superintendência de Segurança da Informação da empresa, que responderam prontamente aos questionários com evidências e documentos. Além disso, percebeu-se que a empresa possui forte preocupação com a área de Defesa. A coordenação do setor cibernético no âmbito do Ministério da Defesa está a cargo do Exército Brasileiro, conforme a Diretriz Ministerial do MD nº 14/2009 (BRASIL, 2009). Desta forma, foi ressaltada a importância de uma forte integração da área de segurança da informação do SERPRO e o Exército Brasileiro, através do Ministério da Defesa. Inclusive, o atual Diretor de Operações da empresa, diretoria responsável pela Superintendência de Segurança da Informação, é um general de divisão, veterano do Exército no comando de áreas relacionadas às tecnologias de informação e comunicações, o que demonstrou fortemente esta integração, além da preocupação com a área de Defesa.

O alto grau de maturidade de governança em segurança da informação e governança cibernética que a empresa apresentou, pode também ser reaproveitado em todo o governo federal, além das muitas experiências na área que podem ser compartilhadas com outros órgãos da Administração Pública Federal (APF), concluindo que essa cooperação deve ser cada vez mais efetiva, de forma a ampliar a atuação da E-Ciber nos demais órgãos, especialmente os que possuem baixa maturidade de governança cibernética, apresentando-se assim como um trabalho futuro.

Por fim, gerou preocupação as notícias na imprensa acerca de eventual privatização do SERPRO. Como empresa pública, criada em 1964, representa uma importante reserva de infraestrutura e, especialmente, informação estratégica para o Estado Brasileiro. Na atual era da informação, onde dado é considerado o novo petróleo, e em especial as informações econômico-fiscais, informações de comércio exterior, sistemas de gestão governamental, além do sistema público de escrituração digital, que são informações extremamente sensíveis à democracia brasileira, a efetivação desta privatização tem o potencial de aumentar os riscos ao Brasil, colocando estes dados essenciais à democracia brasileira em poder de uma única

empresa privada, podendo ser estrangeira. Este risco afeta, desde a privacidade dos cidadãos, informações estratégicas do Estado Brasileiro, podendo atingir também sua soberania. Assim, recomenda-se que a privatização desta empresa não seja realizada sem o prévio amplo debate, com a população e com os gestores públicos dos três poderes da República, apresentando especialmente estes potenciais riscos aos dados de todos os brasileiros.

REFERÊNCIAS

BRASIL. Decreto nº 9.203, de 22 de novembro de 2017. **Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional**. Diário Oficial, Brasília, DF, 23 nov 2017. Seção 1.

BRASIL. Decreto nº 9.573, de 22 de novembro de 2018. **Aprova a Política Nacional de Segurança de Infraestruturas Críticas**. Diário Oficial, Brasília, DF, 23 nov 2018a. Seção 1.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. **Aprova a Estratégia Nacional de Segurança Cibernética**. Diário Oficial, Brasília, DF, 06 fev 2020. Seção 1.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal.** Diário Oficial, Brasília, DF, 01 dez 2012. Seção 1.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Diário Oficial, Brasília, DF, 24 abr 2014. Seção 1.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial, Brasília, DF, 15 ago 2018b. Seção 1.

BRASIL. Ministério da Defesa. Diretriz Ministerial nº 14/2009, de 9 de novembro de 2009. **Atribuiu ao Exército Brasileiro a responsabilidade pela coordenação e integração do Setor Cibernético do Ministério da Defesa**. Brasília, DF, MD/EB, 2009.

CERT. **Cartilha de Segurança para Internet**. Disponível em: <https://cartilha.cert.br/>.Acesso em: 12 abr 2020.

CORREIA, Ana Raquel Marinho. **A atuação dos comitês de tecnologia da informação (TI) no direcionamento da governança de TI nos IF's**. – 2017. 171 f. Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Pernambuco, 2017.

CRUZ JÚNIOR, Samuel César. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**, 2013.

LIMA, Milton Vinicius Morais de. **Uma metodologia para avaliar a maturidade das configurações de segurança em ambientes de data center: uma estrutura sistemática com multiperspectiva**, 2017. 168 f. Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Pernambuco, 2017.

MUTHUKRISHNAN, S. M.; PALANIAPPAN, S. **Security metrics maturity model for operational security**. ISCAIE 2016 - 2016 IEEE Symposium on Computer Applications and Industrial Electronics, p. 101–106, 2016.

ROEN, Marcelo Bastos**. Os Desafios Estratégicos para a Defesa e Segurança Cibernética: Um Estudo de Caso na Administração Pública Federal**. 2017. 118 f. Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Pernambuco, 2017.

SÊMOLA, Marcos. **Gestão da Segurança da Informação - Uma Visão Executiva. Rio de Janeiro**: Elsevier, 2014.

SERPRO. **Relatório Executivo de Atualização Tecnológica em Segurança da Informação**. 2019a.

SERPRO. **Plano Estratégico de Tecnologia da Informação e Plano Diretor de Tecnologia da Informação**. 2019b.

SERPRO. **Decisão Diretiva RI–124 do comitê estratégico de governança, riscos, controles e segurança da informação**. 2019c.

SERPRO. **Relatório *TrustCheck SpotCheck Assessment* da auditoria Unisys**. 2019d.

VERGARA, S. C. **Projetos e Relatórios de Pesquisa em Administração**. 10ª edição, São Paulo, Atlas, 2009.

ANEXO - Relação de Entrevistas e de Respondentes de Questionários

ENTREVISTADO A. Superintendente de Segurança da Informação do SERPRO. Questionamentos enviados por correio eletrônico e videoconferência em junho de 2020. Respostas obtidas em junho e em julho de 2020.

ENTREVISTADO B. Gerente de Departamento de Segurança da Informação do SERPRO. Questionamentos enviados por correio eletrônico e videoconferência em junho de 2020. Respostas obtidas em junho e em julho de 2020.

ENTREVISTADO C. Gerente do Departamento de Gestão de Segurança da Informação e de Continuidade de Negócios do SERPRO. Questionamentos enviados por correio eletrônico e videoconferência em junho de 2020. Respostas obtidas em junho e em julho de 2020.

ENTREVISTADO D. Gerente de Departamento de Segurança da Informação do SERPRO. Questionamentos enviados por correio eletrônico e videoconferência em junho de 2020. Respostas obtidas em junho e em julho de 2020.