ANÁLISE DE PADRÕES DE SEGURANÇA DA INFORMAÇÃO E PRÁTICAS NA GESTÃO DE DADOS NO SEBRAE/PB: PROPOSIÇÃO DE MELHORIAS PARA ELEVAR A SEGURANÇA CIBERNÉTICA ORGANIZACIONAL

JAILMA ARAÚJO DOS SANTOS[1]

WAGNER JUNQUEIRA DE ARAÚJO[2]

RESUMO

No contexto atual, onde os dados são considerados um ativo valioso, as organizações enfrentam um grande desafio que se traduz em como proteger esses ativos, como proteger seus processos de negócios dos crescentes ataques cibernéticos, que visam tornar seus serviços digitais indisponíveis. Tais ataques podem resultar em sequestros de dados, sobrecarregar a infraestrutura computacional da empresa, causar indisponibilidade dos serviços digitais, de modo a impedir que se desenvolva suas atividades. Cabe, portanto, as organizações estarem preparadas e atentas às dimensões da segurança da informação, para a proteção dos ativos tecnológicos e informacionais. O objetivo geral desse trabalho foi: Analisar padrões de segurança da informação, traçar um paralelo com as ações em curso no Sebrae Paraíba, de modo a propor um plano de ação para elevar a segurança cibernética da instituição, contemplando métodos, arquitetura tecnológica, serviços e conhecimentos que minimizem os riscos de ataques cibernéticos em suas camadas de dados. Para atingir tal objetivo foram usadas as seguintes referências: ISO 27000; NIST Cybersecurity Framework; CIS Controls®; Mapas visuais e avaliação de índice de maturidade em segurança do Gartner Group; checklist proposto pelo Conselho Nacional de Justiça (CNJ); Políticas em curso no Sebrae Paraíba. Como resultado da análise foi possível identificar que o Sebrae Paraíba vem implementando políticas, estratégias e soluções de segurança da informação que permitirá a elevação de maturidade na proteção. No entanto, há necessidade de evoluir na implantação de norma de segurança, implementar controles, ampliar as iniciativas de segurança e estender o olhar para os demais ativos de negócios.

Palavras-chaves: Proteção de dados; Segurança da informação; Cibersegurança; Frameworks de segurança.

ANALYSIS OF INFORMATION SECURITY STANDARDS AND DATA MANAGEMENT PRACTICES AT SEBRAE/PB: PROPOSED IMPROVEMENTS TO INCREASE ORGANIZATIONAL CYBER SECURITY

ABSTRACT

In the current context, where data are considered a valuable asset, organizations face a great challenge that translates into how to protect this asset, how to safeguard their business processes from the growing onslaught of cyber-attacks, which aim to render their digital services unavailable. Such attacks can result in data hijackings, that weaken the company's

[1] Especialista em Gestão de Dados no Cenário Big Data | Servidora SEBRAE-PB | E-mail: jailma@pb.sebrae.com.br

[2] Pós doutor em Ciência da Informação | UFPB |E-mail: wagner.junqueira@academico.ufpb.br

relationship with customers, partners, and society. It is therefore up to organizations to be prepared and attentive to the dimensions of information security, for the protection of technological and data assets. The general objective of this project was: To analyze information security standards, to draw a parallel with the current efforts underway at Sebrae Paraíba and to propose an action plan to increase the institution's cyber security by contemplating methods, technology architecture, services and knowledge that minimize the risk of cyber-attacks to its data layers. To achieve this goal, a list of controls for the prevention were used: ISO 27000; NIST Cybersecurity Framework; CIS Controls®; Checklist proposed by the National Council of Justice (CNJ); Gartner Group visual maps and security maturity index assessment; Ongoing policies in Sebrae and Sebrae Paraíba. As a result of the analysis, it was possible to identify that Sebrae Paraíba have been implementing information security policies, strategies and solutions that will allow the increase of maturity in its protection, especially of its data. However, there is a need to elect a security standard and implement established controls, expand security initiatives, and expand the scope to other business assets.

Keywords: Information security management; Data protection; Cybersecurity; Security frameworks; Cyber-attack.

1 INTRODUÇÃO

No cenário atual, as organizações em todo o mundo estão diante de uma demanda crescente de redesenho das estratégias corporativas para que se tornem orientadas a dados ou Data Driven, buscando cada vez mais filtrar, interpretar e utilizar estes dados para apoiar as tomadas de decisões. Este movimento fundamenta-se e estimula que: decisões estejam centradas em análise de dados e inteligência de negócios, sobretudo para capitalizar o exponencial volume de dados produzido atualmente por consumidores, governos, empresas e sociedade como um todo, gerado a partir do Big Data.

Para assegurar a mineração e uso competitivo desses dados como ativos, torna-se fundamental considerar os 5 V's do Big Data: Volume, Velocidade, Variedade, Veracidade e Valor (MCAFEE, BRYNJOLFSSON, 2012; DEMCHENKO et al., 2013), somados aos estágios do Ciclo de Vida de dados, que correspondem a Privacidade, Integração, Qualidade, Direitos Autorais, Disseminação e Preservação (SANT'ANA 2016).

O Sebrae é uma instituição na qual todas as suas iniciativas de relacionamento com clientes e sociedade possuem ricas bases de dados, informação, e conhecimento como núcleos. Assim, a empresa destaca no seu mapa estratégico objetivos que levam as equipes à uma cultura de análise e orientação a dados, materializada por um conjunto de competências, programas e projetos, a exemplo do Programa Nacional de Inteligência de dados.

O presente trabalho tem como foco as linhas de atuação: Proteção de Dados e Privacidade - PDP, bem como Arquitetura de Dados, como ferramentas adequadas para "ANÁLISE DE PADRÕES DE SEGURANÇA DA INFORMAÇÃO E PRÁTCAS NA GESTÃO DE DADOS NO SEBRAE/PB: Proposição de melhorias para elevar a segurança cibernética organizacional". E está inserido no Programa Nacional de Inteligência de dados.

2 OBJETO DE ESTUDO

De acordo com os dados levantados pelo FortiGuard Labs, laboratório de inteligência de ameaças da empresa, em 2021, o Brasil ocupou o segundo lugar em número de ataques cibernéticos na América Latina e Caribe, atrás apenas do México (com 156 bi) e na frente de Peru (11,5 bi) e Colômbia (11,2 bi). A alta nos números foi constante durante o ano de 2021 e ocorreu em toda a região, que chegou a registrar 289 bilhões de ataques no total, um crescimento de mais de 600 por cento, com relação ao ano de 2020 (com 41 bi). (TI INSIDE, 2022, *Online*)

É imperativo ressaltar que uma das dimensões fundamentais nos processos de gerenciamento de dados é a de gestão da segurança da informação. Sem esta camada, dados e informações estarão extremamente vulneráveis, tanto do ponto vista das relações legais, quanto da exposição a ataques cibernéticos, bem como às ações de sequestros de dados que comprometam as estratégias e operações em curso.

Dispor de recursos, serviços e tecnologias que garantam disponibilidade de dados e plataformas que neutralizem tentativas de ataques, sequestros de dados e uso indevido de informações são requisitos essenciais para todas as organizações, uma vez que grande parte dos seus processos e serviços são transacionados por meio digital. Tendo em foco que é crescente o número de ataques cibernéticos e de sequestros de dados em todo o país.

A presente pesquisa nasce então da necessidade de analisar o nível de adoção de padrões de segurança no Sebrae Paraíba, que minimizem riscos de ataques cibernéticos em suas camadas de dados.

3 OBJETIVOS

Os objetivos estabelecidos no trabalho foram:

- **Analisar padrões de segurança da informação, traçar um paralelo com as ações em curso no Sebrae Paraíba, de modo a propor um plano de ação para elevar a segurança cibernética da instituição**, contemplando métodos, arquitetura tecnológica, serviços e conhecimentos que minimizem os riscos de ataques cibernéticos em suas camadas de dados.
- Mapear padrões normas e diretrizes de segurança cibernética de dados.
- Levantar riscos, ameaças e vulnerabilidades em segurança cibernética de dados.
- Elaborar uma proposição de plano de ação para elevar a segurança cibernética do Sebrae Paraíba.

3.1 Gestão de dados

Os dados são elementos estruturantes para a composição de informações, conhecimentos e competências em uma organização, assim como para o desenvolvimento, oferta de produtos e serviços que tenham valor percebido por consumidores e sociedade.

> Todas as organizações precisam de dados e algumas indústrias dependem muito dele. Bancos, companhias de seguros, serviços públicos e órgãos governamentais como a Receita Federal e a Administração de Seguridade Social são exemplos óbvios. A manutenção de registros está no centro dessas "culturas de dados "e o gerenciamento efetivo de dados é essencial para o seu sucesso (DAVENPORT, 2017. p. 16).

As organizações, visando otimizar processos, aproximar-se dos clientes e melhorar resultados, estão efetuando grandes mudanças nas dimensões: pessoas, processos e tecnologias. Nesse sentido, se faz necessário atuar com foco na sustentação da evolução dos negócios. Esta evolução está fortemente centrada na orientação a dados, nas tecnologias digitais, bem como nas novas formas de relações de interação e trabalho.

> O gerenciamento de dados é um conjunto de práticas adotadas para lidar com todas as informações coletadas e geradas por uma empresa de maneira segura e efetiva, considerando todas as políticas e regulamentos de dados. Ao coletar, manter e utilizar dados de maneira correta a empresa é capaz de oferecer suporte a aplicativos de missão crítica, impulsionar análises avançadas e possibilitar eficiências operacionais em tempo real, enquanto reduz os custos de infraestrutura (IBM, 2021).

A Gestão de Dados do Sistema Sebrae tem como objetivo viabilizar por meio do conjunto das funções de dados que ela contempla: o desenvolvimento, execução e supervisão de planos, políticas e práticas que fornecem, controlam, protegem e aumentam o valor dos dados e informações ao longo de seus Ciclos de Vida. "Os ativos de dados na era da informação são de total importância para as organizações, e são vitais para as empresas que querem se impor no mercado" (AIKEN, 2014, p.39).

O Sebrae Paraíba tem como bases originárias dos seus produtos e serviços a informação e o conhecimento, tanto para os pequenos negócios, como sobre estes atores da economia, os quais compõem a imensa maioria de empresas em todo o país. Tal é a importância do tema, que o novo posicionamento estratégico do SEBRAE destaca como prioridade a evolução para uma organização orientada a dados (DataDriven).

E neste cenário que o avanço tecnológico e o crescimento exponencial do volume de dados produzidos a cada dia têm proporcionado o surgimento de um novo tipo de empresa, onde as aplicações e processos orientados por dados, ancorados fortemente nos recursos de big data, analytics e inteligência artificial, são a principal fonte de inovação e geração de valor.

A instituição compreende que a tomada de decisão baseada em dados se torna a cada dia mais necessária, para que assim entregue evolução e inovação para os negócios, permitindo as equipes filtrar, interpretar, investigar problemas e gerar soluções na velocidade em que o atual cenário demanda.

Para assegurar disponibilidade, integridade e confidencialidade dos dados, atributos que conduzem as ações de proteção destes ativos, faz necessário contar com metodologias, serviços e tecnologias de segurança da informação.

4 SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

Para estabelecer uma abordagem holística da proteção de dados, é fundamental explorar os domínios da segurança da informação. A segurança da informação está diretamente relacionada à preservação do valor de dados e informações, tanto de pessoas, quanto de negócios.

De acordo com o TCU, A segurança de informações visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela

instituição. A integridade, a confidencialidade e a autenticidade de informações estão intimamente relacionadas aos controles de acesso. (TCU, 2017)

O conceito de Segurança da Informação, estabelecido no Decreto Nº 9.637, de 26 de dezembro de 2018, destaca que, Segurança da Informação, em modo resumido, "abrange a Segurança Cibernética, a Defesa Cibernética, a Segurança Física e a Proteção de Dados Organizacionais e as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação".

Especialistas destacam 8 (oito) áreas da segurança da Informação nas quais as empresas precisam implantar controles e práticas de proteção: Gestão de Acesso e Identidade, Inteligência contra ameaças, gestão de vulnerabilidades, gestão de risco, gerenciamento de riscos de terceiros, resposta a incidentes, segurança das operações/defesa cibernética, recuperação de desastres em TI, continuidade dos negócios e segurança de aplicações.

É importante destacar ainda o conceito de Ativo de Informação. A definição de um ativo na norma ABNT NBR ISO/IEC 27002 destaca que Ativo é qualquer coisa que tenha valor para a organização.

Manter atenção e conformidade às normas de segurança em todos os ativos é essencial para garantir a disponibilidade dos serviços digitais, vez que uma falha, especialmente em ativos físicos(hardware), de software, e de serviços, pode comprometer a realização de atividades e rotinas corporativas, bem como causar impacto na proteção de dados e informações.

Neste sentido, se faz necessário observar também as diretrizes estabelecidas na Lei Geral de Proteção de Dados Pessoais (LGPD), relevantes e obrigatórias para a coleta, processamento e armazenamento de dados pessoais. "A legislação se fundamenta em diversos valores e tem como principais objetivos:" ("ANS e LGPD - LinkedIn")

> Assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, por meio de práticas transparentes e seguras, garantindo direitos fundamentais. ("O que muda com a nova Lei de Dados Pessoais? - LGPD")
> Estabelecer regras claras sobre o tratamento de dados pessoais.
> Fortalecer a segurança das relações jurídicas e a confiança do titular no tratamento de dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo. ("Conheça LGPD - Sebrae")
> Promover a concorrência e a livre atividade econômica, inclusive com portabilidade de dado (SEBRAE, 2021)

No Sebrae Paraíba e nas organizações como um todo, as estratégias e ações de segurança da informação convergem para proteção dos dados, tanto aqueles originados das rotinas e dos processos de gestão internos (planejamento, orçamento, compras e contratações, finanças, contabilidade, pessoal etc.), como aqueles originados das transações e relacionamento com o cliente.

Logo, é fundamental que os serviços de segurança da informação contemplem soluções que assegurem conformidade com a LGPD, tais como: "Serviço de prevenção contra vazamento de informações; Mapeamento e descoberta de dados pessoais e sensíveis; Consentimento de cookies; anonimização e proteção de dados, respostas aos incidentes de segurança e de privacidade" (SEBRAE,2021).

5 NORMAS E PADRÕES DE SEGURANÇA DA INFORMAÇÃO / PROTEÇÃO DE DADOS

A Governança e operação da TI em relação a gestão de segurança da informação, está conectada e estruturada sob um conjunto de normas e padrões nacionais e internacionais, tendo como umas das principais a Lei SarbanesOxley (SOX); As recomendações do COSO(The Comitee of Sponsoring Organizations); O COBIT (Control Objectives for Information and related Technology) e O ITIL (Information Technology Infrastructure Library), somados a novas metodologias de gestão e frameworks, focados em segurança da informação e criados para acompanhar a evolução das relações humanas e de negócios por meio de plataformas digitais, redes sociais e sistemas computacionais cada vez mais abrangentes. Tais documentos são considerados relevantes para fins deste trabalho, e são descritas a seguir:

ISO/IEC 27000

Do conjunto de normas da ISO/IEC 27000, 19 normas integram diretrizes para o Sistema de Gestão de Segurança da informação, em sua quinta edição de 2018:

- ISO 27001 - Especifica os requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar sistemas de Gestão de Segurança da Informação (SGSI) no contexto dos riscos gerais de negócios da organização. (WIKIPEDIA, 2022)

- 27002 - Fornece uma lista de objetivos de controle comumente aceitos e controles de boas práticas a serem usados como orientação de implementação ao selecionar e implementar controles para alcançar a segurança da informação. (WIKIPEDIA, 2022)
- 27003 Diretrizes para implantação de um SGSI. (WIKIPEDIA, 2022)
- 27004 - Fornece diretrizes destinadas a auxiliar as organizações a avaliar o desempenho da segurança da informação e a eficácia do SGSI. (WIKIPEDIA, 2022)
- 27005 - Fornece diretrizes para o gerenciamento de riscos de segurança da informação. A abordagem descrita neste documento suporta os conceitos gerais especificados em ISO/IEC 27001. (WIKIPEDIA, 2022)
- ISO/IEC 27006 - Requisitos para órgãos que fornecem auditoria e certificação de sistemas de gestão de segurança da informação. (WIKIPEDIA, 2022)
- ISO/IEC 27007 — Diretrizes para auditoria de sistemas de gestão de segurança da informação (focada na auditoria do sistema de gestão). (WIKIPEDIA, 2022)
- ISO/IEC 27008 — Orientação para auditores sobre controles de SGSI (com foco na auditoria dos controles de segurança da informação). (WIKIPEDIA, 2022)
- ISO/IEC 27009 — Tecnologia da informação — Técnicas de segurança — Aplicação específica do setor da ISO/IEC 27001 — Requisitos. (WIKIPEDIA, 2022)
- ISO/IEC 27010 - Gerenciamento de segurança da informação para comunicações intersetoriais e intraorganizacionais. (WIKIPEDIA, 2022)
- ISO/IEC 27013 — Diretriz sobre a implementação integrada da ISO/IEC 27001 e ISO/IEC 20000-1. (WIKIPEDIA, 2022)
- ISO/IEC 27014 — Governança de segurança da informação. (WIKIPEDIA, 2022). (WIKIPEDIA, 2022)
- ISO/IEC TR 27016 - economia de segurança da informação. (WIKIPEDIA, 2022).
- ISO/IEC 27017 — Código de prática para controles de segurança da informação com base na ISO/IEC 27002 para serviços em nuvem. (WIKIPEDIA, 2022)
- ISO/IEC 27018 — Código de prática para proteção de informações de identificação pessoal (PII) em nuvens públicas atuando como processadores de PII. (WIKIPEDIA, 2022)

- ISO/IEC 27019 — Segurança da informação para controle de processos no setor de energia. (WIKIPEDIA, 2022)
- ISO/IEC 27021 — Requisitos de competência para profissionais de sistemas de gerenciamento de segurança da informação. (WIKIPEDIA, 2022)
- ISO 27799 — Gerenciamento de segurança da informação em saúde usando ISO/IEC 27002 (orienta organizações do setor de saúde sobre como proteger informações pessoais de saúde usando ISO/IEC 27002). (WIKIPEDIA, 2022)

5.1 NIST *Cybersecurity Framework*

O NIST é responsável pela publicação do NIST Cybersecurity Framework, conjunto de boas práticas que fornece uma estrutura de política de orientação sobre segurança, sobre como as organizações do setor privado podem avaliar e melhorar sua capacidade de prevenir, detectar e responder a ataques cibernéticos. No documento intitulado "Como implementar com sucesso o NIST Cybersecurity Framework, apresenta uma estrutura básica que consiste em cinco funções simultâneas e contínuas — Identificar, Proteger, Detectar, Responder e Recuperar. (GAT InfoSec, 2020)

Quando analisadas em conjunto, essas funções fornecem uma visão estratégica de alto nível do ciclo de vida do gerenciamento do risco de segurança cibernética de uma organização. (GAT InfoSec, 2020)

5.2 CIS Controls®

O CIS (*Center of Internet Security*) é uma organização sem fins lucrativos, voltada para a comunidade de segurança. É responsável pelo CIS *Controls*, práticas recomendadas e mundialmente reconhecidas para proteger aplicações e dados nos ambientes de tecnologia.

A versão atual do *framework* (versão 8) combina e consolida os controles CIS por atividades. Foram atualizados algumas terminologias e agrupamento de salvaguardas, resultando em uma diminuição do número de controles, de 20 (versão 7.1) para 18 (versão 8), quais sejam: CIS *Controls* 1: Inventário e Controle de Ativos Empresariais; CIS *Controls* 2: Inventário e Controle de Ativos de Software; CIS *Controls* 3: Proteção de Dados; CIS *Controls* 4: Configuração segura de ativos e softwares corporativos; CIS *Controls* 5: Gerenciamento de contas; CIS *Controls* 6:

Gerenciamento de Controle de Acessos; CIS *Controls* 7: Gerenciamento Contínuo de Vulnerabilidades; CIS *Controls* 8: Gerenciamento de Log de Auditoria; CIS *Controls* 9: Proteções de e-mail e navegador da Web; CIS *Controls* 10: Defesas contra malware; CIS *Controls* 11: Recuperação de dados; CIS *Controls* 12: Gerenciamento de infraestrutura de rede; CIS *Controls* 13: Monitoramento e Defesa de Rede; CIS *Controls* 14: Conscientização sobre segurança e treinamento de habilidades; CIS *Controls* 15: Gerenciamento de provedores de serviços; CIS *Controls* 16: Segurança de software de aplicativo; CIS *Controls* 17: Gerenciamento de Resposta à Incidentes; CIS *Controls* 18: *Pentest* (Testes de Intrusão) (CIS, 2020).

5.3 Metodologias *Gartner Group*

O Gartner Group por sua vez apresenta 3 documentos que podem nortear ações de segurança da informação, gestão de riscos e proteção de negócios:

5.3.1 Roteiro para a maturidade da segurança da informação para proteger os ativos da empresa. (*Protect business assets with a roadmap form maturing information security*). (GARTNER, INC. 2022)

O grupo destaca que, “Os líderes de segurança e gerenciamento de riscos devem criar e implementar uma visão de segurança da informação que apoie tanto a criação de valor digital em escala quanto a gestão pragmática dos riscos à segurança. O aumento da capacidade de segurança e eficácia depende criticamente da implementação de uma estrutura madura que planeje, arquiteta, reporte e modifique as atividades de segurança, dependendo de fatores internos e externos.” (GARTNER, INC. 2022)

5.3.2 Roteiro para Cibersegurança em TI (The IT Roadmap for Cybersecurity)

Neste documento o grupo propõe um mapa focado na cibersegurança em si, alertando que “A transformação digital de negócios e sistemas cibernéticos emergentes criam riscos de segurança sem precedentes.

A partir de pesquisa especializada e interações com milhares de empresas em todos os setores, o *Gartner Group* compilou as melhores práticas de segurança cibernética em um roteiro personalizável, com as principais etapas, recursos e pessoas necessárias para planejar e executar uma iniciativa eficaz de cibersegurança: Alinhar a estratégia; iniciar a execução; construir e amadurecer programa; Reavaliar e otimizar (GARTNER, INC. 2022)

5.3.3 Análise de maturidade Gartner para segurança e gerenciamento de riscos de TI (Gartner IT Score for Security and Risk Management)

Nessa análise o Gartner procura medir o desempenho da organização em termos de: Maturidade, por meio de uma série de perguntas sim/não sobre como sua função se aproxima e executa cada ação de uma série de atividades e objetivos importantes específicos para sua função. Importância: solicita que indique o quão importante cada uma dessas atividades é para a sua função para atender aos seus objetivos corporativos. (GARTNER, INC. 2022).

5.3.4 PCI DSS *Payment Card Industry Data Security Standard*

A indústria de pagamentos faz uso do PCI DSS. Em resumo apresentado na PagBrasil, a empresa destaca que o padrão foi criado no ano de 2004 pela iniciativa conjunta das bandeiras de cartão Visa, MasterCard, American Express, Discover e JCB.

As iniciais PCI DSS vêm do inglês "*Payment Card Industry Data Security Standard*", ou seja, é o Padrão de Segurança de Dados da Indústria de Pagamento com Cartão, que te como objetivo: "proteger as informações pessoais dos titulares de cartão e, portanto, reduzir o risco de roubo de dados de cartão ou fraude." (PAGBRASIL, 2022).

O Padrão de Segurança de Dados da Indústria de Pagamento com Cartão está composto de doze requisitos agrupados em seis grandes objetivos, apresentados no Quadro 1:

Quadro 1 – PCI DSS – Padrão de Segurança de Dados da Indústria de Pagamento com Cartão

Escalabilidade	Cobertura	Disponibilidade	Acesso	Qualidade
Garantir que a infraestrutura permite que novos stakeholders desfrutem dela é fundamental para manter a empresa empoderada com dados.	- Garantir que todos os dados possíveis relativos à operação da empresa estão sendo corretamente curados/manipulados.	Os dados devem estar disponíveis para serem consultados sempre que algum stakeholder precisar dele.	Garantir que todos os stakeholders têm o acesso correto aos dados, o quanto antes	- Os dados a disposição dos usuários devem estar curados e canonizados

Fonte: PagBrasil (2022)

6 METODOLOGIA

As temáticas apresentadas neste relatório técnico constituem-se como áreas de conhecimento e de gestão que precisam estar cada vez mais presentes em todas as organizações: gestão e proteção de dados, segurança da informação, segurança cibernética, mitigação de riscos nos negócios e evolução na relação com clientes e sociedade.

As metodologias utilizadas foram a pesquisa exploratória, por se tratar de um assunto com transversalidade em toda a governança organizacional; a pesquisa bibliográfica, realizando coleta de informações a partir de testes, dissertações, livros e documentos internos, para fundamentar a temática. E por fim a pesquisa-ação, por ser um relato prático com participação direta da autora em conjunto com as equipes do Sistema Sebrae e Sebrae Paraíba.

O Sebrae Paraíba como recorte espacial de análise disponibilizou seu acervo de informação e conteúdo e assim realizamos o levantamento de informações, dados e pesquisa bibliográfica que permitissem uma maior clareza acerca da segurança da informação e áreas correlatas.

Neste sentido, foi possível estabelecer para o trabalho o seguinte objetivo: Analisar padrões de segurança da informação, traçar um paralelo com as ações em curso no Sebrae Paraíba, de modo a propor um plano de ação para elevar a segurança cibernética da instituição, contemplando métodos, arquitetura tecnológica, serviços e conhecimentos que minimizem os riscos de ataques cibernéticos em suas camadas de dados, fundamentando-se nas seguintes metodologias: ISSO 27000; NIST *Cybersecurity Framework*; CIS *Controls*®; Mapas visuais e avaliação de índice de maturidade em segurança do *Gartner Group*; Políticas em curso no Sistema Sebrae e

Sebrae Paraíba, assim como o Checklist de controles para prevenção e mitigação de ameaças cibernéticas e confiança digital, baseados na ISSO 27000 (CNJ).

6.1 Plano de ação para elevar a segurança cibernética do sebrae paraíba

A elaboração deste plano está fundamentada nos objetivos estratégicos do Sistema Sebrae: INFORMAÇÃO E CONHECIMENTO - Prover infraestrutura de dados para a criação, a transferência e a aplicação do conhecimento com eficiência e TECNOLOGIA - Prover tecnologia adequada para uma constante evolução digital.

Fundamente-se ainda nos seguintes Atos Normativos: Manual do Programa de Compliance; Política de Classificação da Informação; Política de Gestão de Dados Pessoais Política de Gestão de Incidente com Violação de Dados Pessoais; Política de Governança de Proteção de Dados Pessoais e Privacidade;Política de Segurança da Informação e Comunicação

Assim como nas normas e padrões de segurança: ISO/IEC 27000; NIST Cybersecurity Framework; CIS Controls® ; Metodologias Gartner Group; PCI DSS; ITIL - Information Technology Infrastructure Library; COBIT - Control Objectives for Information and Related Technology; Framework COSO

6.2 Justificativa

As organizações, visando otimizar processos, aproximar-se dos clientes e melhorar resultados, estão efetuando grandes mudanças nas dimensões: pessoas, processos e tecnologias. Nesse sentido, se faz necessário atuar com foco na sustentação da evolução dos negócios. Esta evolução está fortemente centrada na orientação a dados, nas tecnologias digitais, bem como nas novas formas de relações de interação e trabalho.

É imperativo ressaltar que uma das dimensões fundamentais nos processos de gerenciamento de dados é a de gestão da segurança da informação. Sem esta camada, dados e informações estarão extremamente vulneráveis, tanto do ponto vista das relações legais, quanto da exposição a ataques cibernéticos, bem como às ações de sequestros de dados que comprometam as estratégias e operações em curso.

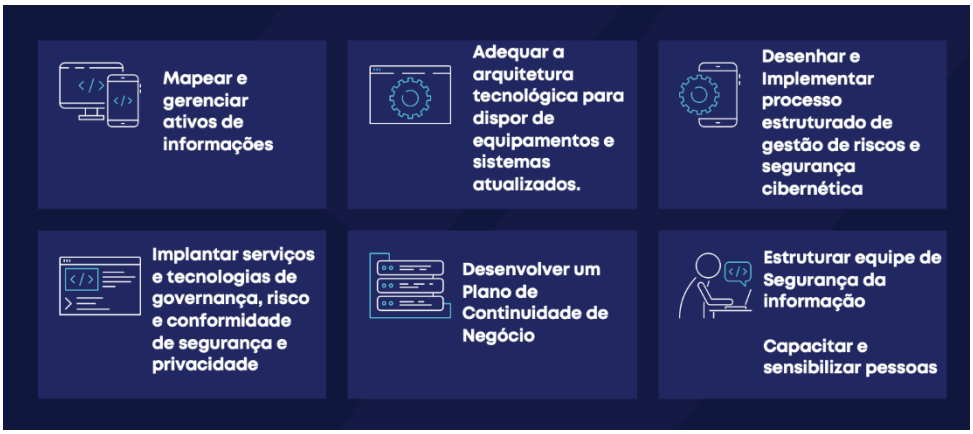
Manter atenção e conformidade às normas de segurança em todos os ativos é essencial para garantir a disponibilidade dos serviços digitais, uma vez que uma falha, especialmente em ativos físicos(hardware), de software, e de serviços, pode comprometer a realização de atividades e rotinas corporativas, bem como causar impacto na proteção de dados e informações.

Seguir, ainda, controles estabelecidos nas normas, ampliar as iniciativas de segurança e estender a segurança para os demais ativos de negócios, entendo a necessidade de proteção em todas as camadas: informação/dados, de software/aplicações, físicos, de serviços, de pessoas e intangíveis.

6.3 Ações Recomendadas

O plano ora proposto configura-se com um instrumento essencial para o Sebrae Paraíba implementar ações, serviços e tecnologias que garantam disponibilidade de dados e plataformas que neutralizem tentativas de ataques, sequestros de dados e uso indevido de informações, uma vez que grande parte dos seus processos e serviços são transacionados por meio digital. Tendo em foco que é crescente o número de ataques cibernéticos e de sequestros de dados em todo o país. As ações recomendadas são apresentadas na Figura 2:

Figura 1 – Ações Recomendadas



Fonte: Elaborada pela autora (2022)

A figura traz ênfase para as seguintes ações:

- Mapear e gerenciar ativos de informações.
- Adequar a arquitetura tecnológica para dispor de equipamentos e sistemas operacionais atualizados, que suportem as necessidades de processamento e

armazenamento de dados corporativos e disponham de recursos de segurança nativos.

- Desenhar e Implementar processo estruturado de gestão de riscos e segurança cibernética, para prevenção e mitigação de ameaças cibernéticas e confiança digital.
- Implantar serviços e tecnologias de governança, risco e conformidade de segurança e privacidade, que assegurem condições de predição, prevenção, detecção e resposta à ataques cibernéticos e demais incidentes de segurança.
- Desenvolver um Plano de Continuidade de Negócio
- Estruturar equipe de Segurança da informação
- Capacitar e sensibilizar constantemente colaboradores e partes interessadas

6.4 Resultados Esperados com o Plano de Ação

- Assegurar proteção de dados e informações do Sebrae PB, por meio de recursos de criptografia, prevenção de vazamento de dados, filtros de segurança nas aplicações acessíveis pela Internet, controle de acesso às aplicações, redes e serviços de TI.
- Garantir disponibilidade dos sistemas, bases e arquivos para que as equipes possam desempenhar as atividades organizacionais.
- Prover segurança na realização de atividades de trabalho.
- Disponibilizar um ambiente monitorado e confiável, dividido em produção, homologação e disponibilidade (backup e replicação).
- Manter proatividade em correções, ajustes e evolução das tecnologias quando necessários.
- Dispor de melhores condições para resposta à incidentes

7 CONSIDERAÇÕES FINAIS

Estar preparado para enfrentar situações críticas em segurança da informação, tais quais as trazidas em um incidente de segurança, carrega consigo o desafio de restabelecer os ativos de informações organizacionais, bem como a oportunidade de reluzir os pontos de fragilidade nas diversas camadas do ciclo de disponibilidade de

serviços de TI. Grande parte destas revelações passam pelas dimensões de segurança da informação.

É fundamental que o Sebrae Paraíba eleja e implante, inicialmente, uma das metodologias de segurança apresentadas neste trabalho, avalie a implantação do plano de ação proposto, somadas a outras estratégias corporativas, objetivando acelerar a disponibilidade de barreiras de proteção da instituição e colocá-la em um nível que ofereça riscos cada vez menores de incidentes e ataques cibernéticos.

É essencial ainda dispor de pessoas para atuar em segurança da informação, desenhar planos e estratégicas, assegurar investimentos, seguir metodologias reconhecidas, capacitar e sensibilizar constantemente colaboradores e partes interessadas de que a segurança da informação é de responsabilidade coletiva e cada ator envolvido precisa garantir o cumprimento dos padrões e regras estabelecidas.

REFERÊNCIAS

AIKEN, P. **A função do chief data officer:** redefinindo as diretorias executivas para se beneficiar do seu mais valioso ativo. – 1.ed. – Rio de Janeiro: Elsevier. [S.l.], 2014. 39

CNJ. Conselho Nacional de Justiça. **Manual de referência – Prevenção e mitigação de ameaças cibernéticas e confiança digital**. CNJ. [S.l.], 2021. 39. Disponível em: https://www.cnj.jus.br/wpcontent/uploads/2021/03/AnexoVManualReferenciaPrevencaoMitigacaoDeAmeacasCiberneticasConfiancaDigitalRevisadoREV.docx.pdf Acesso em: 02 de jun. 2022.

DAVENPORT, J. G. H. T. H. **Competing on analytics:** Updated, with a new introduction: The new science of winning. Harvard Business Press. [S.l.], 2017. 16, 39

DAVENPORT, J. G. HARRIS, R. M. T**. H. Analytics at work:** Smarter decisions, better results. Harvard Business Press. [S.l.], 2010. 39

DAVENPORT, T. H. **Big Data At Work:** Dispelling The Myths, Uncovering The Opportunities. Harvard: Harvard Business School Publishing. [S.l.], 2014. 39

GARTNER. O roteiro de TI para segurança cibernética. 2021.Disponível em: https://www.gartner.com/en/information-technology/trends/the-it-roadmap-for-cybersecurity?utm_medium=asset&utm_campaign=RM_GB_YOY_ITRDMP_WT_LP1_MTURINGINFOSEC&utm_term=ebook (Acessível por meio de login e senha) Acesso em: 12 de jun. 2022.

IBM Cost of a Data Breach Report, 2021

PAGBRASIL. **O que é o PCI DSS e quais são seus requisitos?** 2017. Disponível em: https://www.pagbrasil.com/pt-br/insights/pci-dss-requisitos/ Acesso em: 26 de jun. 2022.

SANT'ANA, R. C. G. Ciclo de vida dos dados: uma perspectiva a partir da Ciência da Informação. **Informação**. *v.21, n.2, p.116-142*. [S.l.], 2016. 11, 39

WIKIPEDIA. **ISO.** Disponível em: https://en.wikipedia.org/wiki/ISO/IEC_27000-series Acesso em: 31 de jul. 2022.