CAMPUS PORTO VELHO ZONA NORTE

CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS PARA INTERNET

INGRID SALETE OLIVEIRA ALVES

MARIA ELIZABETE DA SILVA COSTA

SEGURANÇA DA INFORMAÇÃO:

ATUAÇÃO PROFISSIONAL NA PREVENÇÃO E RESPOSTA A INCIDENTES NA ADMINISTRAÇÃO PÚBLICA

PORTO VELHO/RO

2024

INGRID SALETE OLIVEIRA ALVES
MARIA ELIZABETE DA SILVA COSTA

SEGURANÇA DA INFORMAÇÃO:
ATUAÇÃO PROFISSIONAL NA PREVENÇÃO E RESPOSTA A INCIDENTES NA ADMINISTRAÇÃO PÚBLICA

Artigo apresentado ao Curso Superior de Tecnologia em Sistemas para Internet so Instituto Federal de Educação, Ciência e Tecnologia de Rondônia – IFRO Campus Porto Velho Zona Norte como requisito avaliativo para obtenção do título de Tecnólogo em Sistemas para Internet.

Orientador: Prof. Esp. Tiago Lopes de Aguiar.

PORTO VELHO/RO

2024

Ficha catalográfica elaborada pelo Sistema Gerador de Ficha Catalográfica do IFRO, com dados informados pelo(a) próprio(a) autor(a).

Alves, Ingrid Salete Oliveira.
Segurança da Informação: atuação profissional na prevenção e resposta a incidentes na administração pública / Ingrid Salete Oliveira Alves, Maria Elizabete da Silva Costa, Porto Velho-RO, 2024.
17 f.

Orientador(a): Prof. Esp. Tiago Lopes Aguiar.

Trabalho de Conclusão de Curso (Superior de Tecnologia em Sistemas para Internet) – Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO, Porto Velho-RO, 2024.

1. Segurança da informação. 2. Setor público. 3. Estratégias para mitigação de riscos. 4. Resposta a incidentes. I. Costa, Maria Elizabete da Silva. II. Aguiar, Tiago Lopes (orient.). III. Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO. IV. Título.

Bibliotecário(a) Responsável: Gizele de Melo Viana, CRB-CRB11/914 (Campus Porto Velho Zona Norte)

CAMPUS PORTO VELHO ZONA NORTE
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS PARA INTERNET

SEGURANÇA DA INFORMAÇÃO: atuação profissional na prevenção e resposta a incidentes na administração pública

Ingrid Salete Oliveira Alves[1], Maria Elizabete da Silva Costa[2], Tiago Lopes de Aguiar[3]

RESUMO: O presente artigo procura revelar como a administração pública está se organizando para prevenir e responder a incidentes de segurança da informação por meio da adequada atuação de profissionais da área, observando as estratégias empregadas para garantir a continuidade das operações de negócios. Foi desenvolvido por meio do estudo de caso no âmbito da Superintendência Estadual de Tecnologia da Informação e Comunicação – SETIC do Governo do Estado de Rondônia, realizando-se entrevistas semiestruturadas com especialistas em segurança da informação, bem como revisão bibliográfica, esta última utilizada para revelar as recomendações doutrinárias na área e compará-las com as práticas identificadas. A análise qualitativa dos dados revelou que a implementação de ferramentas técnicas e a criação de comitê multidisciplinar especializado em resposta a incidentes são fundamentais para aprimorar a segurança e a resiliência organizacional. Além disso, a capacitação contínua dos colaboradores se mostra essencial para mitigar ameaças cibernéticas. Essas práticas são cruciais para proteger os dados e garantir a confiança dos cidadãos nos serviços públicos digitais, destacando a SETIC como um modelo a ser seguido no setor público.
Palavras–chave: Segurança da informação. Setor público. Estratégias para mitigação de riscos. Resposta a incidente.

INFORMATION SECURITY: Professional Practices in Preventing and Responding to Incidents in the Public Sector

ABSTRACT: This article aims to reveal how public administration is organizing to prevent and respond to information security incidents through the effective role of professionals in the field, examining strategies employed to ensure the continuity of business operations. It was developed through a case study within the State Superintendency of Information and Communication Technology (SETIC) of the Government of the State of Rondônia, conducting semi-structured interviews with information security specialists, as well as a literature review, the latter used to uncover doctrinal recommendations in the field and compare them with identified practices. Qualitative data analysis revealed that the implementation of technical tools and the creation of a multidisciplinary committee specialized in incident response are essential to enhance security and organizational resilience. Furthermore, continuous staff training is crucial to mitigate cyber threats. These practices are essential to protect data and ensure citizen trust in digital public services, highlighting SETIC as a model to be followed in the public sector.

[1] Discente do Curso Superior de Tecnologia em Sistemas para Internet do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia, Campus Porto Velho Zona Norte. Lattes: https://lattes.cnpq.br/4481175132493460. E-mail: ingrid.salete@estudante.ifro.edu.br.
[2] Discente do Curso Superior de Tecnologia em Sistemas para Internet do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia, Campus Porto Velho Zona Norte. Lattes: http://lattes.cnpq.br/1285463905714346. E-mail: maria.e@estudante.ifro.edu.br.
[3] Docente do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia, Campus Porto Velho Zona Norte. Especialista em Gestão e Governança de Tecnologia da Informação. Lattes: http://lattes.cnpq.br/8744775169659538. E-mail: tiago.aguiar@ifro.edu.br.

Keywords: Information Security. Public Sector. Risk Mitigation Strategies. Incident Response.

1. INTRODUÇÃO

Na era digital contemporânea, caracterizada pela rápida evolução tecnológica e um fluxo contínuo de dados, a segurança da informação se torna um aspecto crucial para a proteção de dados e do bem-estar das pessoas. Nesse contexto, os profissionais de segurança da informação desempenham um papel fundamental na defesa contra vazamentos de dados e no gerenciamento de incidentes de segurança que podem afetar indivíduos e instituições.

Esses especialistas enfrentam desafios significativos devido à complexidade das infraestruturas tecnológicas e ao aumento dos ataques cibernéticos. Incidentes de vazamento de dados, onde informações sensíveis são expostas, destacam as vulnerabilidades críticas no ecossistema digital. Tais eventos, muitas vezes envolvendo extensos volumes de dados, colocam em risco a segurança dos dados e da privacidade das pessoas, além de levantar sérias questões sobre as estratégias de segurança e sobre as políticas de proteção de dados existentes.

No setor público, a segurança da informação assume um papel crítico devido à vasta quantidade de dados que as instituições governamentais armazenam. A digitalização dos serviços públicos e o aumento das interações *online* entre cidadãos e governo tornam os dados e informações vulneráveis a ataques cibernéticos. Isso exige uma abordagem rigorosa e prioritária para protegê-las, buscando garantir a privacidade dos cidadãos e a continuidade dos serviços essenciais. A falta de proteção adequada pode comprometer não apenas a confiança dos usuários dos serviços, mas também a integridade das operações públicas, resultando em graves consequências para a administração.

O presente estudo visa explorar como os profissionais de segurança da informação abordam e gerenciam esses desafios. Concentra-se em entender as práticas adotadas para prevenir e responder a incidentes de segurança, examinando as estratégias de mitigação de riscos e a eficácia das respostas a tais incidentes. A questão central deste trabalho investiga: como os profissionais de segurança da informação no setor público previnem e respondem a incidentes de segurança?

O objetivo é revelar as práticas correntes, destacar os desafios enfrentados pelos profissionais de segurança da informação do setor público e avaliar as estratégias de segurança implementadas para proteger as informações. Este estudo pretende contribuir para um entendimento mais aprofundado das dinâmicas de segurança da informação na era digital, fornecendo *insights* que possam orientar o desenvolvimento de práticas corporativas

responsáveis e ações conscientes, visando a proteção da privacidade e a segurança dos dados em uma sociedade cada vez mais informatizada.

2. REFERENCIAL TEÓRICO

2.1. Segurança da Informação

A segurança da informação (SI) procura garantir a proteção de dados em ambientes corporativos, públicos ou privados. Ela abrange políticas, práticas e tecnologias destinadas a proteger as informações contra acessos não autorizados, alterações indevidas e perdas, acidentais ou intencionais. Fontes (2006) explica que a segurança da informação é composta por normas e orientações que têm como objetivo proteger esse recurso e assegurar o funcionamento eficiente das atividades institucionais. À medida que as organizações se tornam cada vez mais dependentes das Tecnologias da Informação e Comunicação (TICs), a necessidade de aprimorar constantemente essas medidas de proteção se torna evidente, diante do crescimento das ameaças e da complexidade das infraestruturas digitais.

A SI se baseia em três princípios essenciais, conhecidos como Modelo CID:

- Confidencialidade: assegura que apenas pessoas autorizadas possam acessar as informações, evitando sua divulgação sem permissão prévia (Fernandes, 2013);
- Integridade: garante que os dados permaneçam exatos e imunes a alterações não autorizadas, preservando sua precisão (Fernandes, 2013); e
- Disponibilidade: assegura que as informações estejam acessíveis quando necessário, possibilitando o correto funcionamento de sistemas e redes (Fernandes, 2013).

Esses três princípios são interdependentes e formam a base de qualquer estratégia de segurança, para manter a confiança e a eficiência operacional das entidades.

Compreender os princípios da SI é importante para proteger os dados. No entanto, para garantir uma gestão eficaz, é necessário distinguir as definições de ameaças, vulnerabilidades e riscos. Esses conceitos interligados ajudam as organizações a estruturar suas defesas de forma proativa.

2.2. Diferença entre ameaças, vulnerabilidades e riscos

Na segurança da informação, compreender as distinções entre ameaças, vulnerabilidades e riscos é essencial para uma gestão eficaz da segurança. Estes conceitos,

embora inter-relacionados, possuem definições e implicações distintas que influenciam na forma como uma organização se protege contra potenciais incidentes de segurança.

Uma ameaça pode ser entendida como qualquer circunstância ou evento com o potencial de causar danos a um sistema ou organização. As ameaças são inerentes ao ambiente em que a organização opera e podem se manifestar de diversas formas, como ataques cibernéticos, desastres naturais, ou até mesmo erros humanos. A ameaça, portanto, é algo externo à organização que, caso se concretize, pode comprometer a confidencialidade, integridade ou disponibilidade das informações (Agra; Barboza, 2019).

Já a vulnerabilidade é uma fragilidade ou deficiência presente nos sistemas, processos ou controles de uma organização, que pode ser explorada por uma ameaça. As vulnerabilidades são como brechas que, quando descobertas por um agente malicioso, podem ser usadas para causar danos. Elas podem ser resultadas de falhas na configuração de sistemas, *software* desatualizado, ou mesmo a ausência de políticas de segurança adequadas. A vulnerabilidade, portanto, reside internamente na organização e representa uma porta de entrada para a materialização de uma ameaça (Agra; Barboza, 2019).

O risco, por sua vez, emerge da interação entre ameaças e vulnerabilidades. Ele pode ser definido como a probabilidade de que uma ameaça explore uma vulnerabilidade e cause impacto negativo à organização. O risco é, portanto, uma medida que combina a gravidade da vulnerabilidade com a probabilidade de ocorrência da ameaça, e as consequências que isso pode trazer. A gestão de riscos é uma prática essencial na segurança da informação, pois permite que a organização priorize e trate as vulnerabilidades mais críticas, mitigando as ameaças mais prováveis de se concretizar (Barreto, 2018).

Em resumo, enquanto a ameaça é um perigo potencial e externo, a vulnerabilidade é uma fraqueza interna explorável, e o risco é a probabilidade de tal exploração ocorrer e afetar a organização. Para garantir que seja possível implementar medidas de segurança adequadas e proteger a organização contra possíveis incidentes, é vital compreender essas distinções.

Conhecendo tais conceitos, as organizações precisam se preparar para agir de forma rápida e eficaz diante de incidentes de segurança da informação. Nesse contexto, os Grupos de Resposta a Incidentes de Segurança da Informação (CSIRTs) são fundamentais, oferecendo uma abordagem estruturada para detectar, mitigar e responder a incidentes cibernéticos, assegurando a continuidade dos negócios.

2.3. Grupo de Resposta a Incidentes de Segurança da Informação

Os Grupos de Resposta a Incidentes de Segurança da Informação (CSIRTs) são equipes especializadas que atuam na detecção, análise, resposta e mitigação de incidentes de segurança cibernética. Inicialmente, surgiram como uma resposta às ameaças crescentes ao ambiente digital, sendo uma estratégia fundamental para proteger a integridade, confidencialidade e disponibilidade dos dados nas organizações.

De acordo com Killcrece (2003), um CSIRT é definido como uma organização ou equipe que trabalha para a prevenção de incidentes de segurança computacional, com a finalidade de receber, avaliar e responder a notificações relacionadas a incidentes de segurança. Estes grupos desempenham um papel preventivo, semelhante ao de equipes de emergência, buscando não apenas responder a crises, mas também prevenir ocorrências futuras por meio de medidas proativas. O conceito de CSIRT tem se expandido globalmente, com diversas variações adaptadas às necessidades específicas de empresas e governos, oferecendo uma camada essencial de proteção contra ataques cibernéticos.

Os CSIRTs têm como objetivo principal garantir a segurança da informação por meio da identificação rápida de vulnerabilidades e da mitigação de danos. Além disso, proporcionam uma resposta coordenada aos incidentes, o que é fundamental para a recuperação e contenção eficazes contra ataques. Conforme a definição do First (2019), os CSIRTs oferecem uma gama de serviços, como gestão de incidentes e vulnerabilidades, análise forense e disseminação de conhecimento para toda a organização. Essas equipes também são responsáveis por elaborar relatórios pós-incidente, fundamentais para o aprimoramento contínuo dos processos internos e para a implementação de melhores práticas de segurança. A importância dos CSIRTs na manutenção da estabilidade das operações e na preservação dos dados de uma organização é inegável, sendo uma estrutura que visa assegurar tanto a resposta quanto a prevenção de incidentes cibernéticos (Cert.br, 2024).

A eficácia dos CSIRTs depende da atuação dos profissionais de segurança da informação, que implementam políticas e coordenam respostas a incidentes, garantindo que vulnerabilidades sejam tratadas e mitigadas de forma eficiente, assegurando a integridade dos dados e operações.

2.4. Profissional de Segurança da Informação

O profissional de segurança da informação tem uma função estratégica na proteção das infraestruturas tecnológicas e dos dados sensíveis de uma organização. Suas atribuições envolvem a elaboração, implementação e gestão de políticas de segurança que garantam a

integridade, confidencialidade e disponibilidade das informações. Esse papel inclui a coordenação de respostas a incidentes e a mitigação de riscos, sempre alinhado às regulamentações e normas vigentes (GSI, 2020).

Para desempenhar suas funções com excelência, o profissional de segurança da informação deve buscar certificações reconhecidas internacionalmente, como a *Certified Information Security Manager (*CISM), que aborda áreas cruciais como governança, gestão de riscos e conformidade (Behaviour Group, 2013), e a *Certified Ethical Hacker* (CEH), que foca em técnicas de identificação e correção de vulnerabilidades antes que sejam exploradas por agentes maliciosos (EC-Council, 2023). Complementarmente, a certificação LPIC-3 (*Linux Professional Institute Certification* - Level 3) aprofunda o conhecimento em criptografia e segurança em sistemas baseados em Linux, contribuindo para uma defesa mais robusta (Grupo Utah, 2021).

Além do domínio técnico, as competências interpessoais são fundamentais para o sucesso do profissional de segurança da informação. A habilidade de comunicar conceitos complexos de forma acessível, tanto para equipes técnicas quanto para a gestão, é indispensável. Igualmente, a capacidade de liderar equipes e tomar decisões rápidas em momentos de crise reflete a necessidade de equilíbrio entre habilidades técnicas e gerenciais (Cudi-Cdr, 2004).

A atuação desse profissional vai além da simples implementação de ferramentas de segurança. Ele é responsável por desenvolver uma visão estratégica que integre a segurança à missão organizacional, antecipando-se a ameaças emergentes e garantindo a resiliência operacional. Assim, sua capacidade de coordenar ações preventivas e reativas em incidentes de segurança é central para a continuidade dos negócios, minimizando os impactos de possíveis ataques (GSI, 2020; Cudi-Cdr, 2004).

Portanto, o profissional de segurança da informação, ao alinhar certificações de alta relevância com uma atuação estratégica e bem fundamentada, contribui diretamente para a sustentação das operações e para a proteção dos ativos digitais das organizações.

Entre os maiores desafios enfrentados pelos profissionais de segurança da informação estão os vazamentos de dados. Esses incidentes podem expor informações sensíveis, impactando negativamente a organização. Portanto, prevenir e responder rapidamente a vazamentos é uma prioridade central para esses especialistas.

2.5. Superintendência Estadual de Tecnologia da Informação e Comunicação

A Superintendência Estadual de Tecnologia da Informação e Comunicação (SETIC) foi criada pela Lei Complementar nº 965, de 20 de dezembro de 2017, com o objetivo de coordenar e executar as políticas de tecnologia da informação e comunicação (TIC) no Governo do Estado de Rondônia. A SETIC atua como principal órgão responsável por gerir a infraestrutura tecnológica dos órgãos públicos estaduais, assegurando a continuidade e a modernização dos serviços públicos por meio da aplicação de soluções tecnológicas inovadoras. A superintendência é vinculada diretamente à governança digital do estado, sendo uma peça-chave na implementação de políticas que promovem a eficiência, transparência e a inovação no âmbito da Administração Pública Estadual (SETIC, 2017).

De acordo com o artigo 114-A da Lei Complementar Estadual nº 965/2017, a SETIC tem como responsabilidade a coordenação integrada dos sistemas de informação dos diversos órgãos e entidades do estado. Ela promove a padronização e a segurança dos processos tecnológicos, atuando no desenvolvimento e na manutenção de sistemas de informação que suportam as atividades administrativas e operacionais dos órgãos públicos. Além disso, a SETIC é incumbida de garantir a proteção e a segurança dos dados geridos pelo estado, assegurando o cumprimento das normas de confidencialidade, integridade e disponibilidade das informações. A criação de uma infraestrutura de comunicação confiável é fundamental para a prestação eficiente dos serviços públicos e para a transparência na gestão dos recursos estatais.

A SETIC também tem a função de planejar e executar iniciativas que visem a transformação digital do estado, facilitando a adoção de novas tecnologias e melhorando a prestação de serviços aos cidadãos. Ela trabalha na promoção da interoperabilidade entre os sistemas governamentais, o que permite a integração das diferentes bases de dados e sistemas, tornando os processos administrativos mais ágeis e eficientes. Dessa forma, a SETIC contribui para o aumento da transparência e da eficiência administrativa, ao mesmo tempo em que assegura que os serviços oferecidos à população sejam mais acessíveis e confiáveis.

A superintendência desempenha ainda um papel central na gestão da segurança da informação, sendo responsável por implementar políticas e medidas preventivas contra ataques cibernéticos e outras ameaças digitais. Com a evolução constante das tecnologias e a crescente digitalização dos serviços públicos, a SETIC se posiciona como uma entidade estratégica para garantir que o estado de Rondônia esteja preparado para enfrentar os desafios do ambiente digital, sempre com foco na proteção dos dados e na eficiência dos sistemas de comunicação governamentais. Através de suas ações, a SETIC fortalece a governança digital no estado e assegura que a administração pública opere de maneira segura e eficiente.

3. METODOLOGIA

O presente estudo adotou uma abordagem qualitativa com o objetivo de analisar as práticas correntes dos profissionais de segurança da informação do setor público quanto à adoção de estratégias para proteger os dados e informações, utilizando-se como subsídio a coleta e interpretação de informações bibliográficas e de entrevistas. Quanto ao método procedimental, foi adotado o monográfico, consistindo no estudo de caso da Superintendência Estadual de Tecnologia da Informação e Comunicação (SETIC) do Governo do Estado de Rondônia, procurando identificar a atuação profissional de segurança pública no âmbito governamental. A pesquisa se classifica como exploratória, pois busca compreender as estratégias adotadas pelos profissionais de segurança da informação na administração pública.

A delimitação do tema, quanto ao setor público, justifica-se pela crescente relevância da proteção de dados e sistemas no setor público, onde a preservação da integridade, confidencialidade e disponibilidade de informações é crucial. A administração pública lida com grandes volumes de dados, incluindo informações pessoais dos cidadãos, o que a torna um alvo frequente de ciberataques. Nesse contexto, a atuação de profissionais especializados em segurança da informação torna-se indispensável para a criação de barreiras eficazes contra ameaças cibernéticas e a rápida resposta a incidentes, minimizando os impactos dessas ocorrências.

A escolha da SETIC como órgão de referência para realização do presente estudo se deu pelo fato de ser o órgão responsável pela Tecnologia da Informação e Comunicação no Governo do Estado de Rondônia e também por ser referência em segurança da informação e proteção de dados pessoais em âmbito nacional, conquistando do 2º lugar em pesquisa nacional, que avaliou o nível de maturidade em Segurança da Informação (SI), e em Lei Geral de Proteção de Dados Pessoais (LGPD), realizada, através de processo interno, pela Associação Brasileira de Entidades Estaduais de Tecnologia da Informação e Comunicação (Abep-TIC) (SETIC, 2023).

Para a coleta de dados, foram realizadas entrevistas semiestruturadas com dois profissionais da Superintendência Estadual de Tecnologia da Informação e Comunicação (SETIC) do Governo do Estado de Rondônia, ambos servidores públicos efetivos e estáveis, responsáveis pela gestão da segurança da informação em suas respectivas áreas, sendo eles:

- Gabriel Carrijo Bento Teixeira, Diretor Técnico e Analista em Tecnologia da Informação e Comunicação; e
- Leonardo Courinos Lima da Silva, Coordenador de Segurança da Informação e Analista em Tecnologia da Informação e Comunicação.

As entrevistas foram conduzidas de forma individual e guiadas por um roteiro previamente elaborado, com perguntas que exploravam temas relacionados à formação acadêmica, experiências com incidentes de segurança e as políticas de mitigação de riscos. Essas entrevistas permitiram obter *insights* sobre os principais desafios enfrentados no setor público e as soluções aplicadas para lidar com a gestão de vulnerabilidades e incidentes de segurança da informação. As perguntas encontram-se disponíveis no apêndice deste artigo.

Os dados obtidos nas entrevistas foram analisados qualitativamente, com a categorização temática das respostas. Essa abordagem permitiu identificar padrões de comportamento, práticas recorrentes e áreas de melhoria na gestão da segurança da informação. Os resultados foram comparados com as melhores práticas recomendadas na literatura, de modo a avaliar a eficácia das estratégias adotadas e as possíveis lacunas no processo de mitigação de riscos.

Embora o número de entrevistados seja limitado, os dados coletados refletem a realidade de uma organização pública de grande relevância no contexto estadual, o que proporciona uma base sólida para a análise. As limitações quanto à generalização dos resultados são reconhecidas e serão abordadas em detalhes na seção de discussões.

4. RESULTADOS E DISCUSSÕES

É notório a percepção do aumento dos riscos informáticos e a consequente exposição a estes, que afetam tanto instituições públicas quanto privadas. Com o avanço tecnológico, vulnerabilidades em sistemas e redes são exploradas de forma cada vez mais sofisticada, desafiando as defesas das organizações. Conforme observa Sêmola (2014), a crescente complexidade do ambiente digital exige estratégias de defesa adaptáveis e robustas, que, além do uso de tecnologias adequadas, demandam uma cultura organizacional focada na conscientização e na preparação contínua para enfrentar os desafios emergentes.

Nas organizações, a Segurança da Informação (SI) desempenha um papel estratégico, pois vai além da proteção de dados e sistemas, abrangendo também a preservação da reputação e da confiança institucional. Em um ambiente onde há troca de informações, é fundamental garantir a proteção contra acessos não autorizados, interrupções e vazamentos de

dados. Para que essas proteções sejam efetivas, é necessário que as políticas de segurança sejam claras e que as ferramentas de prevenção, monitoramento e resposta a incidentes sejam aplicadas de forma correta (Fontes, 2006). Além disso, a capacitação contínua dos colaboradores sobre suas responsabilidades em relação à SI contribui para um ambiente de trabalho seguro e alinhado às melhores práticas do setor.

Os resultados indicam que, além da implementação de políticas de gestão de incidentes, a capacitação contínua dos colaboradores foi essencial para manter a equipe preparada diante das ameaças cibernéticas. Os treinamentos anuais sobre a Política de Segurança da Informação (PSI) e a LGPD têm sido determinantes para garantir o alinhamento com as melhores práticas do setor, colaborando com a conscientização dos servidores e colaboradores.

A atuação estratégica dos profissionais de segurança da informação vai além do uso de ferramentas e tecnologias. Ela envolve a criação de um ambiente organizacional que incentive a conscientização e a prevenção de incidentes. Como aponta Triplett (2022), o comportamento humano é o ponto mais frágil na segurança digital, o que torna essencial o envolvimento ativo dos líderes com suas equipes para promover boas práticas no dia a dia. A SETIC tem aplicado essas abordagens com sucesso, o que não só fortaleceu sua capacidade de resistir a ameaças, mas também aumentou a confiança nos serviços públicos digitais oferecidos pelo governo.

Nesse contexto, a maturidade da segurança da informação nas organizações não se dá de forma instantânea. Trata-se de um processo contínuo de evolução, que depende tanto da aplicação das tecnologias quanto da conscientização dos profissionais. A cultura organizacional de segurança deve ser reforçada por políticas de gestão bem estabelecidas e pela adaptação constante às ameaças emergentes, que desafiam diariamente a capacidade das organizações de proteger seus ativos.

Para consolidar os aspectos da segurança da informação nas organizações, um dos critérios mais importantes a serem observados é o amadurecimento cultural. No decorrer das entrevistas, constatou-se que a SETIC percorreu uma trajetória de amadurecimento das práticas de segurança da informação no setor público do Governo do Estado de Rondônia. Inicialmente, a organização enfrentava diversos desafios, como a ausência de uma governança clara em SI, conforme relataram os entrevistados. Essa falta de estrutura vai ao encontro do conceito de vulnerabilidade discutido por Agra e Barboza (2019), que destacam como a ausência de políticas de segurança e tecnologias adequadas pode deixar as instituições expostas a ataques cibernéticos.

O incidente mais significativo mencionado foi o ataque de *defacement* em 2019, que serviu como catalisador para a criação da Coordenadoria de Segurança da Informação na SETIC. Essa iniciativa de resposta e coordenação interna reflete a necessidade de equipes dedicadas para gerenciar e mitigar incidentes cibernéticos, conforme descrito por Killcrece (2003). A criação desse comitê foi um avanço crucial para a estrutura de segurança da organização. O *defacement* é uma forma de ataque cibernético em que tanto a aparência quanto o conteúdo de um site são alterados, comprometendo sua integridade e disponibilidade.

Outra iniciativa importante foi a implementação de instrumentos como o Plano de Gestão de Incidentes e o Plano de Continuidade de Ativos de TI, que foram essencial para que a SETIC se preparasse para lidar com crises e falhas em sistemas, indo ao encontro das melhores práticas de governança em segurança da informação discutidas por Fontes (2006). Essas políticas definem claramente as etapas a serem seguidas em caso de incidentes, contribuindo para a resiliência organizacional. A SETIC disponibiliza esses planos e outros documentos relacionados à segurança da informação em sua página de *compliance* (conformidade), onde estão organizadas todas as normativas de segurança, governança e privacidade de dados, facilitando o acesso às informações necessárias para garantir a continuidade e a segurança dos sistemas (wiki.setic.ro.gov.br).

A SETIC possui um comitê de privacidade e segurança da informação que atua como um CSIRT, desempenhando funções de resposta a incidentes de segurança da informação. Esse comitê, que opera há dois anos, se reúne quando ocorrem incidentes de segurança, definindo as atividades a serem realizadas e a função de cada membro. Composto por profissionais de diversas áreas, como banco de dados, segurança, infraestrutura e jurídico, o comitê garante uma resposta integrada e eficaz aos incidentes, refletindo as melhores práticas de gestão. Embora o comitê ainda não tenha uma formalização completa como CSIRT, suas funções e a colaboração entre as equipes indicam um avanço significativo na coordenação e rapidez das respostas a incidentes.

Outra questão importante na SI é a evolução contínua das tecnologias e o surgimento de novas ameaças, o que reflete na necessidade de atualização constante dos equipamentos e sistemas objetivando mitigar os riscos associados. Os entrevistados esclareceram que houve a recente adoção do *Extended Detection and Response* (XDR), uma ferramenta de detecção e resposta avançada que foi fundamental para bloquear um ataque recente que poderia ter causado danos significativos. Essa capacidade de identificar e mitigar vulnerabilidades em

tempo real é uma prática essencial para evitar a exploração dessas brechas (Agra e Barboza, 2019).

Além das ferramentas tecnológicas, a capacitação contínua dos colaboradores foi identificada como uma medida fundamental para manter a equipe alinhada com as práticas de segurança. A SETIC promove treinamentos anuais sobre a Política de Segurança da Informação (PSI) e a Lei Geral de Proteção de Dados Pessoais (LGPD), complementando essas iniciativas com parcerias externas. Essas ações educacionais, conforme recomendado por Fontes (2006), são indispensáveis para garantir que os colaboradores compreendam as normas e estejam preparados para responder a incidentes de segurança da informação de maneira eficaz.

Os entrevistados enfatizaram que a área de segurança da informação exige constante atualização e estudo. Eles destacaram que é necessário acompanhar novas formas de ataque e contaminação que surgem diariamente. Um dos pontos principais foi o estudo de protocolos de rede, como o modelo TCP/IP e o modelo OSI, que são vistos como a base da segurança da informação. Compreender profundamente o funcionamento das comunicações de rede é essencial para avançar para técnicas mais complexas.

Certificações na área de segurança, como as oferecidas pela CompTIA e pela IC Consul em *Ethical Hacking*, foram mencionadas como diferenciais importantes. Além disso, o domínio de *Python* foi destacado como uma habilidade essencial, dada sua versatilidade na automação de tarefas e na análise de vulnerabilidades.

Nesse contexto, os profissionais de segurança da informação desempenham um papel essencial para que as organizações continuem evoluindo e se mantendo seguras. Esses especialistas procuram garantir que as operações do dia a dia sigam sem interrupções e protegem dados importantes contra ameaças. Além disso, são responsáveis por criar estratégias para reduzir riscos, resolver incidentes de forma rápida e garantir que a empresa ou instituição siga as normas e regulamentos. Como destaca Triplett (2022), liderar na área de cibersegurança não é só sobre tecnologia, mas também sobre entender as pessoas e criar processos que ajudem a reduzir erros humanos, o que é uma parte fundamental do trabalho desses profissionais.

Assim, pode-se concluir que os profissionais de segurança da informação da Superintendência Estadual de Tecnologia da Informação e Comunicação (SETIC) têm adotado uma postura proativa na prevenção e resposta a incidentes de segurança. Por meio da implementação de tecnologias avançadas, criação de comitês especializados e investimentos contínuos na capacitação dos colaboradores, a SETIC tem conseguido melhorar suas práticas

de gestão de incidentes, demonstrando uma crescente maturidade em suas operações. Essas ações destacam a importância de uma abordagem estratégica e coordenada para lidar com as ameaças cibernéticas no setor público.

5. CONSIDERAÇÕES FINAIS

O presente estudo revelou a importância das práticas de segurança da informação na administração pública, especialmente no contexto da SETIC do Governo de Rondônia. A implementação de políticas adequadas, aliada à modernização tecnológica, demonstrou ser uma estratégia eficaz para a proteção de dados sensíveis e para o fortalecimento da resiliência organizacional frente às ameaças cibernéticas. Essas práticas se mostraram fundamentais para garantir a continuidade dos serviços públicos digitais e a confiança da população.

A análise dos resultados também evidenciou a importância de se investir continuamente em tecnologia e inovação para melhorar as respostas a incidentes e mitigar riscos. A criação de uma infraestrutura sólida e a adoção de soluções tecnológicas avançadas são passos essenciais para enfrentar os desafios de segurança da era digital. Além disso, a coordenação entre diferentes setores da SETIC foi fundamental para a aplicação das medidas de segurança de forma eficiente e integrada.

Outro aspecto relevante observado foi a necessidade de fortalecer a cultura organizacional de segurança da informação. Para alcançar isso, é imprescindível que líderes incentivem a conscientização e promovam boas práticas de segurança no cotidiano dos colaboradores. A criação de um ambiente que valorize a prevenção e a capacitação contínua é vital para garantir que as equipes estejam preparadas para enfrentar as ameaças emergentes.

Por fim, recomenda-se que futuras pesquisas explorem como outras instituições públicas podem adotar as boas práticas identificadas neste estudo, ampliando o debate sobre a segurança da informação no setor público. A comparação com outras organizações pode fornecer insights valiosos sobre como melhorar as estratégias de proteção de dados e garantir a continuidade dos serviços digitais em diferentes contextos administrativos.

REFERÊNCIAS

AGRA, Andressa D.; BARBOZA, Fabrício F M. **Segurança de sistemas da informação**. Porto Alegre: Grupo A, 2019. E-book. ISBN 9788595027084. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595027084/. Acesso em: 31 ago. 2024.

BARRETO, Jeanine S.; ZANIN, Aline; MORAIS, Isabelly S.; e outros. **Fundamentos de segurança da informação**. Porto Alegre: Grupo A, 2018. E-book. ISBN 9788595025875. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595025875/. Acesso em: 31 ago. 2024.

BEHAVIOUR GROUP. **Certified Information Security Manager (CISM)**. 2013. Disponível em: https://www.behaviour-group.com/PT/wp-content/uploads/kalins-pdf/singles/certified-information-security-manager-cism.pdf. Acesso em: 6 set. 2024.

CERT.br. Grupos de Segurança e Resposta a Incidentes (CSIRTs) Brasileiros. Disponível em: https://www.cert.br/csirts/brasil/. Acesso em: 15 set. 2024.

CUDI-CDR. **Perfil do Oficial de Segurança da Informação**. 2004. Disponível em: https://cudi.edu.mx/rfc/drafts/draft4.pdf. Acesso em: 6 set. 2024.

EC-COUNCIL. **Certified Ethical Hacker (CEH)**. 2023. Disponível em: https://www.eccouncil.org/wp-content/uploads/2023/09/CEH-brochure.pdf. Acesso em: de set. 2024.

FERNANDES, N. (2013) **Segurança da Informação**. Cuiabá- MG, Instituto Federal Rondônia. Disponível em: https://proedu.rnp.br/bitstream/handle/123456789/1538/15.6_versao_Finalizada_com_Logo_I%20FRO-Seguranca_Informacao_04_04_14.pdf?sequence=1. Acesso em: 15 set. 2024.

FIRST. **Computer Security Incident Response Team (CSIRT) Services Framework**. 2019. Disponível em: https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0 bugfix 1.pdf. Acesso em: 15 set. 2024.

FONTES, Edison. **Segurança da informação**: o usuário faz a diferença. 1ª edição. São Paulo: Saraiva, 2006.

GSI, Gabinete de Segurança Institucional. **Perfil do cargo de Diretor de Segurança da Informação**. 2020. Disponível em: https://www.gov.br/gsi/pt-br/composicao/departamento-de-seguranca-da-informacao/perfis-e-curriculos/perfil-do-cargo-de-diretor-de-seguranca-da-informacao. Acesso em: 6 set. 2024.

GRUPO UTAH. **LPIC-3 – 303-200 Enterprise Security**. 2021. Disponível em: https://www.grupoutah.com.br/wp-content/uploads/2021/06/em_lpic_303.pdf. Acesso em: 6 set. 2024.

KILLCRECE, **Georgia et al. State of the Practice of Computer Security Incident Response Teams (CSIRTs)**. 2003. Disponível em:

https://resources.sei.cmu.edu/asset_files/TechnicalReport/2003_005_001_14204.pdf. Acesso em: 15 set. 2024.

SÊMOLA, M. (2014) **Gestão de segurança da informação**: uma visão executiva. 2.ed. Rio de Janeiro: Elsevier. Disponível em: http://wiki.stoa.usp.br/images/archive/7/79/20170827173359%21Cap1-semola.pdf. Acesso em: 15 set. 2024.

SETIC. **Conquista do 2º lugar em Pesquisa Nacional evidencia ações da Tecnologia da Informação do Governo de RO**. 2024. Disponível em: https://rondonia.ro.gov.br/conquista-do-2o-lugar-em-pesquisa-nacional-evidencia-acoes-da-tecnologia-da-informacao-do-governo-de-ro/. Acesso em: 11 out. 2024.

SETIC. **Governo do Estado alcança índice elevado de maturidade na adequação à LGPD**. 2023. Disponível em: https://rondonia.ro.gov.br/governo-do-estado-alcanca-indice-elevado-de-maturidade-na-adequacao-a-lgpd/. Acesso em: 9 out. 2024.

SETIC. **Lei Complementar nº 965, de 20 de dezembro de 2017**. Dispõe sobre a organização e estrutura do Poder Executivo do Estado de Rondônia e dá outras providências. Disponível em: http://ditel.casacivil.ro.gov.br/COTEL/Livros/Files/LC965%20-%20COMPILADA...pdf. **Acesso** em: 7 out. 2024.

SUPERINTENDÊNCIA ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (SETIC). **Plataforma de Documentação Técnica e Gerencial.** Disponível em: https://wiki.setic.ro.gov.br/. Acesso em: 9 out. 2024.

FILHO. Marcos Vinícius Alves e Silva. **Entrevista relativa à investigação de crimes cibernéticos concedida ao acadêmico de Direito Tiago Lopes de Aguiar.** Porto Velho: DRACO, 9 abr. 2018.

TRIPLETT, W. J. **Addressing Human Factors in Cybersecurity Leadership.** ***Journal of Cybersecurity and Privacy*****.** 2022. Disponível em: https://www.mdpi.com/2624-800X/2/3/29. Acesso em: 13 out. 2024.

APÊNDICE ÚNICO – QUESTIONÁRIO APRESENTADO NA ENTREVISTA COM OS PROFISSIONAIS DA ÁREA DE SEGURANÇA DA INFORMAÇÃO DA SETIC

1. Qual o seu cargo e função desempenhada?
2. Qual a sua formação acadêmica e profissional?
3. Você possui alguma certificação técnica na área de informática?
4. Quais foram os principais desafios relacionados à segurança da informação que você vivenciou até o momento no seu ambiente de trabalho?
5. Já se deparou com algum incidente de segurança? Se sim, como foi tratado?
6. Existe algum Grupo de Resposta a Incidentes de Segurança da Informação no seu ambiente de trabalho? Como esse grupo funciona?
7. Quais políticas ou normas de governança em segurança da informação existem no seu ambiente de trabalho?
8. O seu ambiente de trabalho incentiva o treinamento e desenvolvimento contínuo em segurança da informação?
9. Quais as suas recomendações para quem deseja seguir carreira na área de segurança da informação?