AVALIAÇÃO DE MATURIDADE DE EQUIPES DE RESPOSTA A INCIDENTES: UMA PROPOSTA DE MELHORIA A PARTIR DA UTILIZAÇÃO DO SIM3 (SECURITY INCIDENT MANAGEMENT MATURITY MODEL)

EVALUATION OF INCIDENT RESPONSE TEAMS' MATURITY: A PROPOSAL FOR IMPROVEMENT THROUGH THE USE OF SIM3 (SECURITY INCIDENT MANAGEMENT MATURITY MODEL)

Beatriz Barizon Borzi, Fatec Americana, beatriz.borzi@fatec.sp.gov.br
Caroline Valentim Pinto, Fatec Americana, caroline.valentim@fatec.sp.gov.br
Marcus Vinícius Lahr Giraldi, Fatec Americana, marcus.lahr@fatec.sp.gov.br

Resumo

Este artigo tem como objetivo abordar a importância da avaliação da maturidade das equipes de resposta a incidentes, também conhecidas como CSIRTs (*Computer Security Incident Response Teams*), na gestão de incidentes. Para esta avaliação, será utilizado o modelo de autoavaliação *on-line* SIM3 (*Security Incident Management Maturity Model*) da *Open CSIRT Foundation*. Este modelo propõe uma solução prática para ajudar as equipes a identificar áreas que necessitam de melhoria, especialmente em relação aos seguintes quesitos: organização, pessoas, ferramentas e processos. A metodologia utilizada foi a pesquisa bibliográfica e a pesquisa documental. A análise foi baseada em parâmetros e critérios definidos por autoridades internacionalmente reconhecidas no tema, como o *Forum of Incident Response and Security Teams* (FIRST), *The European Union Agency for Cybersecurity* (ENISA) e *Trusted Introducer Service* (TF-CSIRT). Além disso, o artigo discute o papel fundamental da maturidade organizacional na promoção de uma cultura de segurança robusta e a importância de processos contínuos de avaliação para garantir a eficácia das respostas a incidentes de segurança.

Palavras-chave: Avaliação de Maturidade; Equipe de Resposta a Incidentes; *Computer Security Incident Response Teams*; e *Security Incident Management Maturity Model*.

Abstract

This paper aims to address the importance of assessing the maturity of incident response teams, also known as CSIRTs (Computer Security Incident Response Teams), in incident management. To evaluate the teams' maturity, the SIM3 (Security Incident Management Maturity Model) on-line self-assessment model from the Open CSIRT Foundation will be used. This model proposes a practical solution to assist teams in identifying areas that require improvement, especially regarding the following aspects: organization, people, tools, and processes. The methodology used was bibliographic research and document research. The analysis was based on parameters and criteria defined by internationally recognized authorities on the subject, such as the Forum of Incident Response and Security Teams (FIRST), The European Union Agency for Cybersecurity (ENISA) and Trusted Introducer Service (TF-CSIRT). Furthermore, the paper discusses the fundamental role of organizational maturity in promoting a robust security culture

and the importance of continuous evaluation processes to ensure the effectiveness of security incident responses.

***Keywords**: Maturity Assessment; Incident Response Team; Computer Security Incident Response Teams; and Security Incident Management Maturity Model.*

1. Introdução

O uso e a evolução da tecnologia impulsionaram significativamente a produção de dados no ambiente digital. Segundo informações coletadas pela Revista *MIT Technology Review* (2022), estima-se que aproximadamente 2,5 quintilhões de *bytes* de dados são gerados por dia. Esse volume expressivo é resultado de um mundo altamente conectado, onde pessoas e dispositivos estão interligados na originação de novas ideias.

Essas informações são amplamente utilizadas pelas organizações, seja para oferta de bens e/ou serviços, tomada de decisões estratégicas, inovação ou, no caso de empresas privadas, para obtenção de vantagem competitiva. No entanto, assegurar o tratamento e o armazenamento seguro dessas informações é um desafio enfrentado tanto por organizações públicas quanto privadas.

Qualquer comprometimento das informações pode abalar a reputação da organização, além de acarretar responsabilidades legais. Portanto, a equipe de segurança da informação da organização deve fundamentar o tratamento dos dados em três principais pilares: confidencialidade, disponibilidade e integridade.

Um incidente de segurança ocorre quando qualquer um desses pilares é comprometido, seja por um agente interno ou externo, de forma acidental ou intencional. Diante desses eventos não planejados e indesejados, é essencial a preparação de uma equipe capaz de gerenciar a situação - usualmente denominada como *Computer Security Incident Response Team* (CSIRT).

Para avaliação da referida equipe, não basta que a organização tenha controles e normas internas de segurança da informação, a equipe nomeada precisa ser observada no aspecto prático, para verificação de alguns fatores cruciais, como o tempo de resposta, efetividade no tratamento do incidente de segurança, ferramentas disponíveis, entre outros critérios, a fim de mitigar os efeitos advindos da violação ocorrida do modo mais eficiente possível.

O problema central deste estudo reside em como garantir um nível de maturidade recomendado por determinadas autoridades, com relação ao CSIRT, com a finalidade que a organização foque na melhoria contínua, levando em consideração os diversos parâmetros de mercado. O objetivo é assegurar uma resposta a incidentes que atenda às expectativas da organização e dos *stakeholders*.

Para auxiliar as equipes de resposta a incidentes de segurança da informação, apresenta-se, neste artigo, o modelo de autoavaliação *on-line* denominado como *Security Incident Management Maturity Model* (SIM3), disponibilizado pela *Open CSIRT Foundation*.

O intuito da referida ferramenta é a avaliação do nível de maturidade do CSIRT e posterior indicação das melhorias necessárias para atingir um nível de maturidade desejado pela organização com relação à equipe de resposta a incidentes, sendo possível ter resultados baseados nos níveis recomendados pelas principais organizações de cibersegurança em âmbito mundial, como *Forum of Incident Response and Security Teams* (FIRST), *The European Union Agency for Cybersecurity*

(ENISA) e *Trusted Introducer Service* (TF-CSIRT). A obtenção do nível de maturidade recomendado nas avaliações disponibilizadas por essas organizações é considerada como uma boa prática de mercado.

A metodologia de pesquisa adotada é a de abordagem qualitativa e descritiva quanto aos objetivos. Foram realizadas pesquisas bibliográficas e pesquisas documentais para publicação do presente artigo.

O trabalho desenvolvido está dividido em três tópicos. O primeiro tópico tem como objetivo apresentar o aumento de incidentes e a necessidade de uma resposta ao evento indesejado, demonstrando a importância da sua estruturação prévia para eficácia da resposta.

O segundo tópico aborda o funcionamento do CSIRT e suas particularidades e, por fim, o terceiro e último tópico apresenta a solução ainda não tão difundida no Brasil – em especial em pequenas e médias empresas – para avaliação da maturidade das equipes de resposta a incidentes, nomeada como SIM3.

Diante do cenário atual, levando em conta as tecnologias existentes e as emergentes, a coleta massiva de dados, as leis aplicáveis ao tratamento de dados pessoais, a responsabilidade social das organizações e os riscos inerentes à atividade de tratamento de dados, torna-se imprescindível ter uma equipe preparada para responder efetivamente aos incidentes de segurança da informação.

2. Referencial Teórico

2.1. Panorama Tecnológico Atual e a Imperatividade de um Plano de Resposta a Incidentes de Segurança

Atualmente, é um desafio citar o nome de uma organização que não utilize a tecnologia e conexão com outros dispositivos no seu processo de negócio, ainda que seja tão somente na comunicação com os seus clientes e fornecedores ou na realização de atividades internas em rede.

A tecnologia é parte inerente dos negócios na Sociedade Informacional. Manuel Castells (2015, p. 71) pontuou que “O que está surgindo não é uma economia ponto.com, mas uma economia interconectada com um sistema nervoso eletrônico”, e, nesse cenário, “a rede é a empresa” (CASTELLS, 2015, p. 73).

A comprovação da premissa de Castells é facilmente encontrada na variedade de maneiras pelas quais os dados são processados atualmente, conectando bilhões de pessoas e permitindo a coleta massiva de informações e a automatização de tarefas. A evolução de produtos é uma evidência importante da dissolução das “fronteiras tradicionais entre as indústrias. Na área automotiva, o carro agora é um computador sobre rodas, sua parte eletrônica representa aproximadamente 40% do custo de um carro” (SCHWAB, 2019, *e-reader* local 1112 de 3204).

Não só referente aos produtos físicos, é possível ver os exemplos de como a inteligência artificial (IA) permite a inferência de novos dados e automatização de serviços, a internet das coisas (IoT) que possibilita a conexão de objetos tornando a vida mais conectada, entre outras tecnologias emergentes disruptivas.

Toda a inovação, no entanto, não vem sem desafios. A segurança dos dados é um desafio que deve ser enfrentado pelas organizações. Na hipótese de não se obter êxito na proteção da informação, por meio da quebra de qualquer um dos pilares da segurança da informação, tem-se um evento indesejado e não planejado, ou seja, um incidente de segurança.

No cenário atual, à medida que a tecnologia avança e evolui, surgem ameaças e vulnerabilidades até então desconhecidas, aumentando a quantidade de incidentes de segurança, de forma a comprometer dados organizacionais e pessoais, sendo imprescindível responder de forma eficaz e rápida ao se deparar com uma violação de segurança da informação (CICHONSKI, 2012).

A ocorrência de incidentes de segurança é alta, conforme estatística apresentada pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil (2023), conhecido pela sigla CERT.br. Em análise às notificações realizadas de forma voluntária pelas organizações no ano de 2023 ao CERT.br, identificou-se o recebimento, entre os meses de janeiro à março, 160.812 (cento e sessenta mil oitocentos e doze) notificações voluntárias de incidentes de segurança, sendo 74,01% (setenta e quatro e um centésimo por cento) referentes a *scans*, o que inclui notificações de varreduras em redes de computadores, tentativas de ataques de força bruta de senhas, tentativas de exploração de vulnerabilidades, dentre outros ataques já publicados na Internet.

A resposta a incidentes de segurança é um processo complexo, como descrito pelo *National Institute of Standards and Technology* (NIST). O ciclo de vida de um incidente de segurança inclui preparação, identificação e análise, contenção, erradicação, recuperação e atividades pós-evento (CICHONSKI, 2012). Aqui, o CSIRT desempenha um papel vital e a eficácia do CSIRT pode influenciar significativamente em cada etapa deste processo.

Para a resposta a incidentes, é necessária a elaboração de um plano que, segundo Danta (2021, p. 58), deve ser alinhado com as características intrínsecas da organização, considerando aspectos como: missão, visão e valores, estrutura organizacional, segmento de atividade e tipo de negócio.

Danta também ressalta a importância de que o plano seja conhecido por todos na organização, que tenha o apoio da alta administração, e que seja redigido de forma clara e objetiva, apresentando os procedimentos e etapas para guiar a equipe de resposta a incidentes e os envolvidos no incidente, incluindo o que fazer, quem acionar, quais ações são prioritárias e como será comunicada a ocorrência de um incidente de segurança.

Conforme Cichonski et al. (2012) afirmam, em caso de um evento adverso, durante o tratamento de incidentes pode ser fundamental a coleta de informações com o objetivo de aprimorar processos e sistemas internos, mitigar futuros incidentes semelhantes e documentar a experiência e lições aprendidas pela organização.

Somente com um plano de resposta a incidentes é possível minimizar a perda ou o roubo de informações e prevenir interrupções causadas por um incidente, possibilitando o reestabelecimento de serviços e sistemas no menor tempo possível (CERON, 2009).

Por fim, como destacado no Manual do SIM3 pela *Open CSIRT Foundation* (2023), não existe uma solução única que torne uma organização totalmente imune a eventos indesejados. É imprescindível desenvolver medidas para mitigar os riscos, sendo fundamental a formação de uma equipe de resposta a incidentes e o seu constante treinamento a respeito do plano de resposta a incidentes de segurança.

2.2. CSIRTs e sua Relevância para o Contexto Atual

Quando nos referimos à criação de uma equipe de resposta a incidentes, a resposta propriamente dita não é atividade principal, razão pela qual é comum e usual a comparação com a atividade do corpo de bombeiros, cujo objetivo não é apenas extinguir incêndios, mesmo que essa tarefa ganhe visibilidade em momentos de tensão e urgência.

Em ambas as atividades o serviço de qualidade depende da atuação preventiva, realizada por profissionais qualificados e treinados, os quais deverão possuir ferramentas apropriadas para desempenho de suas funções e necessitam ser acionados para tanto.

Johansen (2022, p. 27) ressalta que o corpo de bombeiros realiza o trabalho preventivo, e quando necessária ação de resposta, deve receber a denúncia da população, com a informação da localização do incidente, sua extensão e se há pessoas em perigo. Após a ciência dos fatos, são endereçadas as medidas para lidar com a emergência. A mesma lógica se aplica à equipe de resposta a incidentes.

Nesse sentido é o conceito apresentado por Killcrece et al. (2003), cuja definição do CSIRT consiste em uma organização ou equipe que trabalha para a prevenção de incidentes de segurança de computadores e tem como finalidade receber, avaliar e responder as notificações relacionadas aos incidentes de segurança nas organizações.

Os CSIRTs, segundo Hoepers e Obelheiro (2004), do CERT.br, podem ser de diversos tipos e tamanhos, divididos em: CSIRTs internos, responsáveis por prestar serviços para a organização que os mantém; CSIRTs nacionais, designados para prover o serviço de resposta a incidentes para um país; Centros de Coordenação, que facilitam a comunicação entre vários CSIRTs; Centros de Análises, que definem tendências e padrões ao agrupar informações sobre incidentes; e grupos de empresas fornecedoras, que disponibilizam relatórios de vulnerabilidades de seus produtos de *hardware* e/ou *software.*

O FIRST (2019) menciona uma gama de serviços atrelados ao CSIRT, tais como: gestão de eventos de segurança da informação, gestão de incidentes, gestão de vulnerabilidades, consciência situacional e transferência do conhecimento. É possível que outras atividades sejam inseridas nos serviços acima, como o monitoramento e detecção de incidentes, análise dos eventos por meio de ferramentas automatizadas, análise de evidências forenses, resposta a vulnerabilidades, comunicações internas e externas, e conscientização. Todos estes serviços buscam preservar a confidencialidade, integridade e disponibilidade.

Hoepers e Obelheiro (2004) enfatizam que a conexão entre diversos grupos e organizações é de grande valia para o compartilhamento de informações sobre fraudes, vivências e métodos de resposta a incidentes, sendo um serviço à comunidade.

Ainda, é necessário que os membros do CSIRT entendam todos os processos e áreas da organização, suas ferramentas e sistemas de trabalho, para que, caso necessário, possam agir de forma proativa para a adequação de políticas, realização de conscientização pertinente e até mesmo para utilizar técnicas para identificação de vulnerabilidades, mitigando possíveis incidentes de segurança.

Vale ressaltar a importância de todo esse trabalho. Mesmo a organização que possui a melhor e mais recomendada infraestrutura de tecnologia e segurança da informação, não está imune às ações maliciosas e intrusões de atacantes mal-intencionados, conforme Hoepers e Obelheiro (2004) destacam. Portanto, é de extrema importância que as organizações possuam métodos eficazes de mitigação de segurança da informação, de maneira rápida e eficaz. Esses aspectos serão cruciais para determinar os danos causados e as ações necessárias para a recuperação.

Em um contexto de crescente digitalização e dependência de tecnologias de informação, a presença de um CSIRT se torna cada vez mais indispensável. É uma necessidade que vai além da mera reação a incidentes, alcançando a prevenção e a manutenção de um ambiente seguro. Uma equipe de resposta a incidentes eficaz pode reduzir significativamente o impacto de ataques e intrusões, protegendo a integridade das operações e os ativos de informação da organização.

2.3. A Utilização da Ferramenta SIM3 para Melhoria da Maturidade de Resposta a Incidentes

A *Open CSIRT Foundation* (2019), organização independente sem fins lucrativos, que tem como missão melhorar a resiliência cibernética com o intuito de auxiliar os times de resposta a incidentes, desenvolveu a ferramenta *Security Incident Management Maturity Model* (SIM3). Trata-se de uma avaliação de maturidade que analisa quatro principais pilares de uma equipe de resposta a incidentes, quais sejam: prevenção, detecção, resolução e, por fim, controle de qualidade e *feedback.*

O modelo de avaliação de maturidade foi adotado inicialmente pela TF-CSIRT, organização que promove a colaboração entre CSIRTs da Europa, em maio de 2010, sendo utilizado inicialmente por mais de 200 (duzentas) equipes de resposta a incidentes. Em razão da ampla utilização e importância, posteriormente o modelo contou com a contribuição para melhoria de fóruns globais, como FIRST, CFCE, ITU e transacionais, como AfricaCERT, ENISA, LACNIC, OEA e *Trust Broker Africa*, motivo pelo qual passou por algumas versões (*OPEN CSIRT FOUNDATION ET AL.*, 2023).

A contribuição global permitiu que o modelo de maturidade incorporasse a experiência de diversos profissionais, dos mais diversos tipos organizacionais, os quais possuem vivências distintas, considerando também o país de origem e situações concretas que já enfrentaram. Em suma, a comunidade é de extrema importância para o desenvolvimento de um *framework* que tem como missão ser abrangente e seguir como padrão para organizações de diversos tipos e tamanhos.

Apesar das particularidades de cada organização, o SIM3 recomenda a adoção de medidas gerais para garantir uma abordagem equilibrada e holística, indicando perfis de avaliação, os quais possuem exigências diversas. Uma comunicação eficiente, treinamento contínuo e atualização das habilidades da equipe, bem como a implementação de processos e ferramentas sólidas, são aspectos cruciais para uma gestão de incidentes de segurança eficaz, independentemente do tamanho da organização.

Para auxiliar as organizações, a *Open CSIRT Foundation* (2022) lançou uma ferramenta *on-line* do SIM3, nomeada como SIM3 *Self Assessment Tool*, servindo como um modelo de autoavaliação, facilitando e democratizando o seu acesso, sem a necessidade de investimento financeiro por aqueles que desejam utilizá-la.

O uso do SIM3 tem como resultado esperado a mensuração da capacidade de um time de resposta a incidentes no gerenciamento do incidente, por meio da análise dos pilares de prevenção, detecção, resolução, controle de qualidade e *feedback*, os quais são separados em quatro quadrantes: organização, pessoas, ferramentas e processos.

O resultado é medido por 5 (cinco) parâmetros de maturidade que vão do número 0 ao 4. O parâmetro 0 é adotado quando a organização desconhece o tema ou não definiu nada sobre a questão; o parâmetro 1, quando o conhecimento é implícito, ou seja, apesar de ser conhecido e considerado, não é escrito; o parâmetro 2, quando se trata de conhecimento explícito e interno, mas não formalizado; o parâmetro 3, quando se trata de conhecimento explícito, carimbado ou publicado por uma autoridade do CSIRT; e, por fim, o parâmetro 4, quando é explícito e auditado por autoridade acima do CSIRT (*OPEN CSIRT FOUNDATION et al.,* 2023).

Importante esclarecer que são disponibilizados os resultados com base em 5 (cinco) perfis determinados por comunidades específicas, sendo que cada uma delas define valores mínimos para para que uma equipe seja considerada madura, são elas: *First Membership Baseline*, ENISA/GCMF *Basic*, ENISA/GCMF *Intermediate*, ENISA/GCMF *Advanced* e TI *Certification*.

Para elucidar o que se espera em cada pilar, passa-se a esclarecer os quadrantes utilizados para análise da maturidade das organizações.

2.3.1. Organização

Trata-se da análise da estrutura organizacional, verificando-se a governança no gerenciamento de incidentes de segurança. São considerados aspectos como: estrutura de comando e controle; a definição de papéis e responsabilidades; os recursos disponíveis; e como a organização responde a incidentes de segurança. Ainda, são analisadas as políticas de segurança, a estratégia de gerenciamento de incidentes, as comunicações interna e externa, a gestão de riscos, entre outros (*OPEN CSIRT FOUNDATION et al.,* 2023).

Dentre os 11 parâmetros definidos para avaliação do quesito organização estão: O-1: Mandato; O-2: Constituinte; O-3: Autoridade; O-4: Responsabilidade; O-5: Descrição do Serviço; O-6: Política de Mídia Pública; O-7: Descrição do Nível de Serviço; O-8: Classificação de Incidentes; O-9: Participação em Sistemas CSIRT; O-10: Estrutura Organizacional; e O-11: Política de Segurança (tradução livre).

2.3.2. Pessoas

Um importante ponto de análise são as pessoas da organização, no qual se verifica o gerenciamento de incidentes de segurança interno, o nível de treinamento, a experiência da equipe de resposta a incidentes, a consciência de segurança em toda a organização, bem como a preparação da equipe para desempenhar os papéis definidos (*OPEN CSIRT FOUNDATION et al.,* 2023).

Dentre os 7 parâmetros definidos para avaliação do quesito pessoas estão: H-1: Código de Conduta/Prática/Ética; H-2: Resiliência da Equipe; H-3: Descrição de Habilidades; H-4: Desenvolvimento de Equipe; H-5: Treinamento Técnico; H-6: Treinamento em Habilidades Interpessoais; e H-7: *Networking* Externo. (tradução livre).

2.3.3. Ferramentas

A análise do presente quadrante refere-se às tecnologias e ferramentas utilizadas para detectar, prevenir e responder a incidentes de segurança. São avaliados os requisitos de sistemas de detecção de intrusões, *firewalls*, *software* de análise de logs, e outras ferramentas de segurança cibernética (*OPEN CSIRT FOUNDATION et al.,* 2023).

Dentre os 10 parâmetros definidos para avaliação do quesito ferramentas estão: T-1: Ativos de TI e Configurações; T-2: Lista de Fontes de Informação; T-3: Sistema(s) de Mensagens Consolidadas; T-4: Sistema de Rastreamento de Incidentes; T-5: Chamadas de Voz Resilientes; T-6: Mensagens Resilientes; T-7: Acesso à Internet Resiliente; T-8: Conjunto de Ferramentas para Prevenção de Incidentes; T-9: Conjunto de Ferramentas para Detecção de Incidentes; e T-10: Conjunto de Ferramentas para Resolução de Incidentes (tradução livre).

2.3.4. Processos

Os processos e procedimentos referem-se ao que uma organização possui para gerenciar incidentes de segurança. São analisados processos de resposta a incidentes e elaboração de relatórios, com foco na gestão de incidentes, gestão de mudanças, aprendizado e melhoria contínua (*OPEN*

CSIRT FOUNDATION et al., 2023).

Dentre os 17 parâmetros definidos para avaliação do quesito processos estão: P-1: Escalada para o Nível de Governança; P-2: Escalada para a Função de Imprensa; P-3: Escalada para a Função Jurídica; P-4: Processo de Prevenção de Incidentes; P-5: Processo de Detecção de Incidentes; P-6: Processo de Resolução de Incidentes; P-7: Processos de Incidentes Específicos; P-8: Processo de Auditoria e Feedback; P-9: Processo de Alcançabilidade de Emergência; P-10: Melhores Práticas de Presença na Internet; P-11: Processo de Manuseio Seguro de Informações; P-12: Processo de Fontes de Informação; P-13: Processo de Divulgação; P-14: Processo de Relatórios de Governança; P-15: Processo de Relatórios do Constituinte; P-16: Processo de Reunião; e P-17: Processo de Colaboração entre Pares (tradução livre).

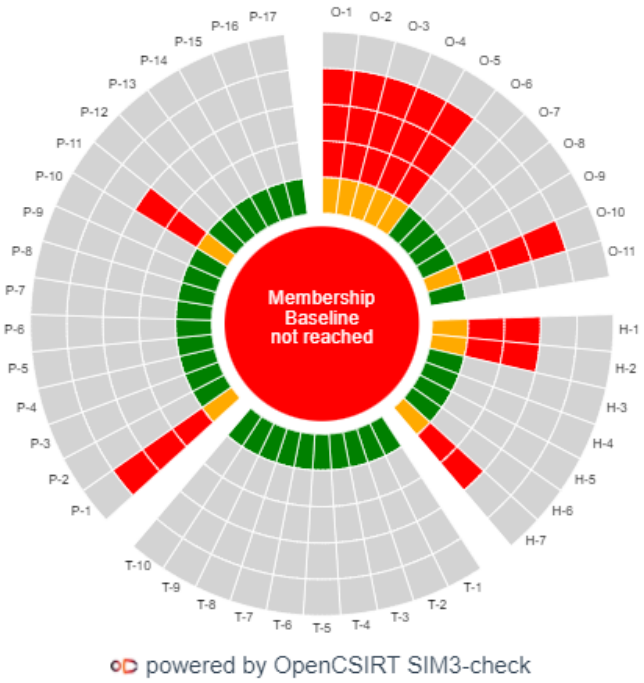
2.4. Cenário Após Resposta da Autoavaliação

Preenchidas todas as questões sobre cada um dos parâmetros supracitados, é gerado um gráfico sobre a avaliação de maturidade, acompanhado de uma planilha de resultados considerando o que é exigido por cada um dos 5 perfis determinados por comunidades específicas, *First Membership Baseline*, ENISA/GCMF *Basic*, ENISA/GCMF *Intermediate*, ENISA/GCMF *Advanced* e TI *Certification,* a fim de apontar as melhorias necessárias e as atividades a serem realizadas para aumento da maturidade da equipe de resposta a incidentes (*OPEN CSIRT FOUNDATION et al.,* 2023).

Além do gráfico, apresenta-se uma tabela de resultados, em formato que permite que seja copiado e inserido em programa de computador para gerenciar tabelas, como o Excel, indicando se há necessidade de melhoria conforme o perfil selecionado, acompanhada das ações em aberto, com a indicação de quais destas estão pendentes para um melhor direcionamento da equipe de resposta a incidentes.

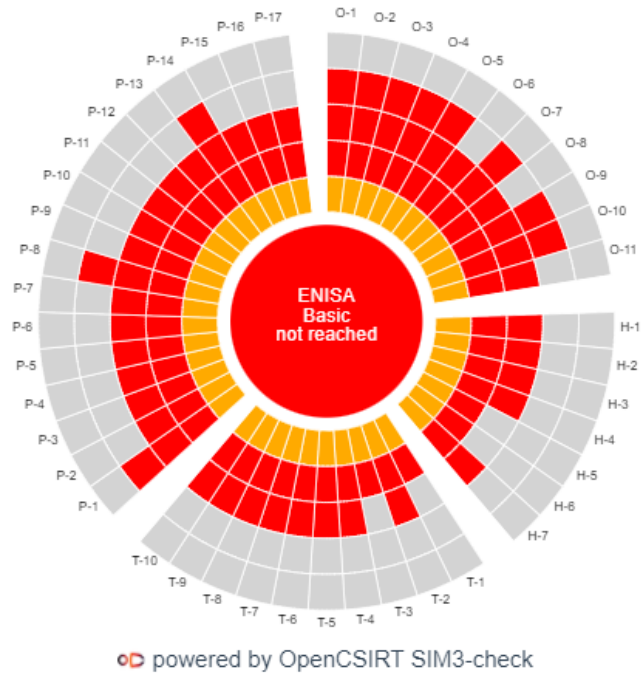
A fim de ser compreendido de maneira visual, as figuras de 1 a 5 representam cada um dos 5 perfis com a definição de todos os parâmetros, em todos os quadrantes, como nível 0, ou seja, a organização desconhece ou não definiu nada sobre o tema. As cores visualizadas no gráfico representam: (i) verde: parâmetros já preenchidos e satisfatórios; (ii) laranja: parâmetro não preenchido e que precisa ser melhorado; (iii) vermelho: parâmetro que precisa ser preenchido para que a organização alcance o nível mínimo para ser classificada em um dos perfis correspondentes (*OPEN CSIRT FOUNDATION* et al., 2023).

Figura 1 – Requisito para se tornar membro do FIRST.



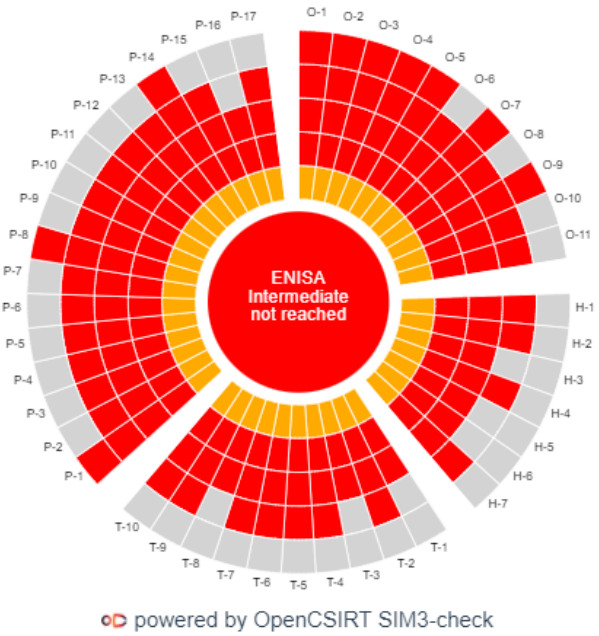
Fonte: *Open CSIRT Foundation* (2023).

Figura 2 – Requisitos para se tornar membro do ENISA *Basic*.



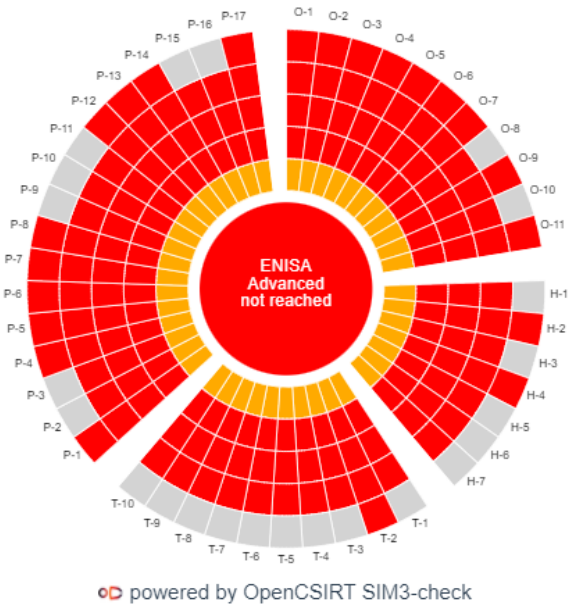
Fonte: *Open CSIRT Foundation* (2023).

Figura 3 – Requisitos para se tornar membro do ENISA *Intermediate*..



Fonte: *Open CSIRT Foundation* (2023).

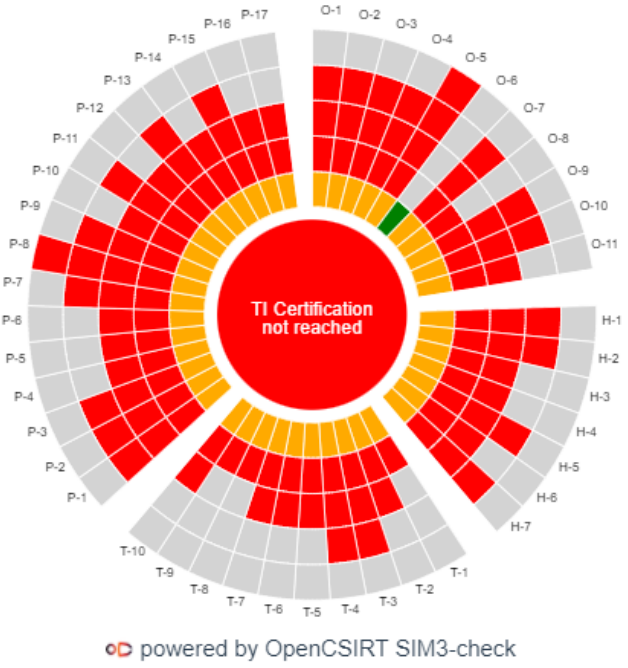
Figura 4 – Requisitos para se tornar membro do ENISA *Advanced*. É possível notar que o nível avançado exige a classificação máxima em 22 dos 45 parâmetros.



Fonte: *Open CSIRT Foundation* (2023).

O gráfico referente à *TI Certification* (Figura 5), certificação destinada a equipes de resposta a incidentes já credenciadas na *Trusted Introducer,* que seguem níveis desejáveis há mais de oito meses, que buscam ter seu nível de maturidade avaliado de forma independente. O processo envolve diversos requisitos adicionais, além das respostas necessárias, tal como *workshop* presencial, e renovação a cada três anos para que as equipes passem por um processo de recertificação (TRUSTED INTRODUCER, 2022).

Figura 5 - Requisitos para participar do processo de certificação do TI *Certification.*



Fonte: Open CSIRT Foundation (2023).

Assim, ao adotar e implementar o SIM3, as organizações podem identificar áreas de melhoria em suas práticas de gerenciamento de incidentes de segurança, aumentar a eficácia de suas equipes de resposta e fortalecer sua postura geral de segurança, reduzindo os riscos de segurança e garantindo uma resposta mais rápida e eficiente a incidentes quando eles ocorrerem.

Ainda, com o resultado, é mais fácil a organização identificar lacunas e pontos fracos nas capacidades de gerenciamento de incidentes de segurança, fornecendo uma base sólida para melhorias contínuas.

Há outros benefícios como *benchmarking* e compartilhamento de melhores práticas em razão de ser utilizada uma base comum para comparar as capacidades de resposta a incidentes entre organizações e setores, aumentando a resiliência e postura de segurança, reduzindo custos e impacto de incidentes etc.

Desse modo, a melhoria das capacidades de gerenciamento de incidentes de segurança pode ajudar a reduzir o tempo de atendimento e a remediar os custos associados a incidentes, bem como a minimizar o impacto de violações de dados e outros eventos de segurança.

3. Metodologia

A fim de atender aos objetivos propostos nesta pesquisa, adotamos uma abordagem qualitativa e descritiva, sustentada por pesquisa bibliográfica e pesquisa documental.

Com relação à revisão bibliográfica, esta foi realizada de forma abrangente para estabelecer uma base teórica sólida. A referida revisão concentrou-se em literatura relevante sobre a avaliação de maturidade, equipes de resposta a incidentes (CSIRTs), e o modelo SIM3. Livros, periódicos acadêmicos e fontes *on-line* foram consultados para fornecer uma visão teórica aprofundada sobre a importância e os desafios da gestão de incidentes de segurança da informação. A pesquisa bibliográfica foi realizada principalmente *on-line*, de agosto de 2022 a maio de 2023.

Em complementação à pesquisa bibliográfica, foi realizada uma pesquisa documental para coletar e analisar documentos relevantes para o estudo. Esses documentos incluem modelo de avaliação de maturidade de equipes de resposta a incidentes, diretrizes e recomendações de organizações de resposta a incidentes como o FIRST, ENISA e Trusted Introducer. Esta pesquisa documental permitiu uma análise realista e baseada em evidências das práticas atuais e desafios enfrentados pelas equipes de resposta a incidentes.

Os dados coletados através das pesquisas bibliográfica e documental foram analisados utilizando uma abordagem qualitativa. Esta análise buscou identificar temas comuns, padrões, e pontos de divergência na literatura existente, bem como explorar o uso prático e a eficácia do modelo SIM3 em contextos do mundo real.

4. Resultados e Discussões

A pesquisa identificou a importância crítica da implementação de uma equipe de resposta a incidentes para garantir os pilares de segurança da informação de qualquer organização. A equipe em questão desempenha um papel fundamental, não apenas na resposta a crises de segurança, mas também na adoção de medidas proativas para prevenir incidentes de segurança.

Foi constatado que modelos e ferramentas, como o SIM3, desenvolvido pela *Open CSIRT Foundation*, são instrumentos valiosos para ajudar as organizações a avaliar e melhorar a maturidade de suas equipes de resposta a incidentes. Esses modelos proporcionam uma análise abrangente dos aspectos relacionados à prevenção, detecção, resolução e controle de qualidade de incidentes de segurança, elevando a postura de segurança na organização, garantindo a resiliência em incidentes futuros, além de aumentar a confiança dos *stakeholders.*

Finalmente, a pesquisa concluiu que a adoção de um sistema de resposta a incidentes, apoiado por ferramentas como o SIM3, é um passo vital para as organizações fortalecerem suas defesas cibernéticas e se prepararem para os desafios de segurança no cenário digital em constante evolução, bem como frente aos desafios regulatórios.

5. Considerações Finais

A implementação de uma equipe de resposta a incidentes é fundamental para a segurança cibernética de qualquer organização. Assim como um corpo de bombeiros não apenas apaga incêndios, mas também trabalha preventivamente para evitá-los, uma equipe de resposta a incidentes não se limita apenas a responder a crises de segurança, mas também adota medidas proativas para prevenir incidentes de segurança.

Diversos modelos e ferramentas, como o SIM3, ajudam as organizações a avaliar e melhorar a maturidade de suas equipes de resposta a incidentes.

A autoavaliação, promovida por essas ferramentas, permite a identificação de áreas de melhoria, a promoção de melhorias contínuas e o compartilhamento de melhores práticas, sem qualquer custo para sua utilização, desde que não haja interesse na certificação da organização.

A implementação de tais modelos e práticas pode resultar em uma postura de segurança mais robusta, aumento da resiliência a incidentes futuros, redução de custos associados a incidentes e ampliação da confiança dos *stakeholders* na capacidade da organização de proteger suas informações e responder efetivamente a incidentes de segurança.

Portanto, recomenda-se a adoção de um sistema de resposta a incidentes, apoiado por ferramentas como o SIM3, que se torna um passo vital para as organizações tornarem suas defesas cibernéticas mais robustas e se prepararem para os desafios de segurança que podem surgir no cenário digital em constante evolução.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Comunicação de Incidentes de Segurança. 2021. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 14 mai. 2023.

CASTELLS, Manuel. A Galáxia da Internet. Trad. Oxford University Press. Rio de Janeiro: Zahar, 2015. E-book. p. 339.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA DO BRASIL. Estatísticas dos Incidentes Reportados ao CERT.br. 2023. Disponível em: https://www.cert.br/stats/incidentes/2019-jan-dec/total.html. Acesso em: 10 mai. 2023.

CERON, Joao et al. O processo de tratamento de incidentes de segurança da UFRGS. 2009. Disponível em: https://www.lume.ufrgs.br/bitstream/handle/10183/16096/000696922.pdf?sequence=1. Acesso em: 19 mai. 2023.

CICHONSKI, Paul et al. Computer Security Incident Handling Guide: recommendations of the national institute of standards and technology. Recommendations of the National Institute of Standards and Technology. 2012. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. Acesso em: 19 mai. 2023.

DANTA, Lígia. Tratamento e Resposta a Incidentes [livro eletrônico]. São Paulo: Editora Senac São Paulo, 2021. E-book. p. 158.

ENISA. Abordagem Gradual de Criação de Uma CSIRT. 2010. Disponível em: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-portugese. Acesso em: 19 mai. 2023.

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_bugfix1.pdf. Acesso em: 19 mai. 2023.

HOEPERS, Cristine; OBELHEIRO, Rafael. CSIRT FAQ. 2004. CERT.br. Disponível em: https://www.cert.br/certcc/csirts/csirt_faq-br.html. Acesso em: 19 mai. 2023.

JOHANSEN, Gerard. Digital Forensics and Incident Response. Birmingham: Packt Publishing Ltd., 2022. p. 511.

KASPERSKY. Quase metade das respostas a incidentes da Kaspersky foram por causa de ransomware. 2022. Disponível em: https://www.kaspersky.com.br/about/press-releases/2022_quase-metade-das-respostas-a-incidentes-da-kaspersky-foram-por-causa-de-ransomware. Acesso em: 19 mai. 2023.

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: 19 mai. 2023.

MIT TECHNOLOGY REVIEW. Data Literacy: a importância da alfabetização em dados em um mundo Big Data. 2022. Disponível em: https://mittechreview.com.br/data-literacy-a-importancia-da-alfabetizacao-em-dados-em-um-mundo-big-data/. Acesso em: 19 mai. 2023.

OPEN CSIRT FOUNDATION ET AL. SIM3: Security Incident Management Maturity Model. 2019. Disponível em: https://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf. Acesso em: 19 mai. 2023.

_____. SIM3 Manual. 2023. Disponível em: https://sim3-check.opencsirt.org/#/. Acesso em: 19 mai. 2023.

_____. SIM3 Self Assessment Tool. 2022. Disponível em: https://sim3-check.opencsirt.org/#/. Acesso em: 19 mai. 2023.

SCHWAB, Klaus. A Quarta Revolução Industrial. São Paulo: Edipro, 2019. E-book. Local 3204.

SKIERKA, Isabel et al. CSIRT Basics for Policy-Makers: the history, types & culture of computer security incident response teams. The History, Types & Culture of Computer Security Incident Response Teams. 2015. Disponível em: https://www.gppi.net/media/Skierka_et_al_2015_CSIRT_Basics_for_Policy-Makers.pdf. Acesso em: 19 mai. 2023.

TRUSTED INTRODUCER. Listing of operational Teams. 2022. Disponível em: https://www.trusted-introducer.org/processes/registration.html. Acesso em: 18 mai. 2023.