Id.: EN34

FRAMEWORK DE SEGURANÇA CIBERNÉTICA PARA REATORES MODULARES PEQUENOS (SMR)

Karytha M. S. Corrêa[1], Joana B. Soares[2], Cássio F. T. da Silva[3], Marcos S. Farias[3], Guilherme D. G. Jaime[3]

[1] Universidade Federal de Minas Gerais (UFMG), Departamento de Engenharia Nuclear, Escola de Engenharia, Av. Antônio Carlos 6627, Cep 31270-901, Belo Horizonte – MG.
[2] Instituto Militar de Engenharia (IME), Praça Gen. Tibúrcio, 80 - Urca, Rio de Janeiro - RJ, 22290-270.
[3] Instituto de Engenharia Nuclear (IEN) - Cidade Universitária, R. Hélio de Almeida, 75 - Ilha do Fundão - RJ, 21941-614.
karymeriesc@ufmg.br

Palavras-Chave: Segurança Cibernética; Acesso Remoto; Gestão de Risco.

RESUMO

O trabalho apresenta o desenvolvimento de um framework nacional de cibersegurança, adaptado especificamente para reatores Small Modular Reactors (SMR), com base em referências reconhecidas como o National Institute of Standards and Technology (NIST), o NEI 08-09 e o Guia Regulatório 5.71. O objetivo é oferecer uma abordagem abrangente e estratégica para aprimorar a segurança cibernética desses sistemas, destacando a importância de seguir práticas seguras e padrões estabelecidos, especialmente em cenários de acesso remoto ao reator. O framework busca proteger os SMRs contra ameaças cibernéticas, garantindo segurança operacional, integridade do sistema e proteção de dados sensíveis. Além de difundir boas práticas de cibersegurança e fortalecer a cultura de segurança nas organizações que operam SMRs, este framework, pioneiro em nível nacional, contribui para o avanço da segurança cibernética em um contexto global, onde os SMRs são uma solução atrativa para atender à crescente demanda de energia de forma segura e sustentável.

1. INTRODUÇÃO

Atualmente, as organizações buscam formas estruturadas e eficientes de lidar com desafios complexos, como a gestão de riscos. Uma ferramenta amplamente utilizada para esse fim é o framework, que se refere a uma estrutura organizacional composta por diretrizes, princípios e boas práticas que ajudam a padronizar e otimizar processos em uma empresa. Um framework oferece um modelo sistemático para identificar, avaliar, mitigar e monitorar ameaças, garantindo uma abordagem consistente e proativa [1],[2].

No contexto da segurança cibernética, a aplicação de frameworks torna-se essencial para mitigar os riscos associados ao crescente uso de tecnologias digitais e à dependência de redes e sistemas informatizados [1],[3]. A cibersegurança é um campo complexo e dinâmico, onde ataques cibernéticos e violações de dados podem causar danos severos a organizações e infraestruturas críticas. Ao implementar frameworks de gestão de riscos de segurança cibernética, as empresas podem estabelecer processos claros para identificar vulnerabilidades, implementar medidas de mitigação, monitorar continuamente seus sistemas e garantir uma resposta ágil e eficaz a incidentes de segurança [1-4].

Um campo que vem ganhando atenção no Brasil, tanto pela inovação quanto pelas preocupações associadas à demanda energética, é o dos Reatores Modulares Pequenos (SMRs – *Small Modular Reactors*). Os SMRs representam uma solução promissora para geração de energia, oferecendo vantagens como flexibilidade operacional e maior segurança em comparação aos reatores nucleares convencionais. Além disso, sua modularidade permite que sejam instalados em áreas remotas, aumentando a viabilidade do uso de energia nuclear em diversas regiões [5]. Em março de 2019, os governos do Brasil e dos Estados Unidos deram início a uma iniciativa de cooperação bilateral denominada Fórum de Energia EUA-Brasil (USBEF) [5]. Uma das

iniciativas acordadas entre os países foi um estudo de avaliação de SMRs para aplicação no Brasil, patrocinado pelo Departamento de Energia dos Estados Unidos e elaborado em parceria com o Idaho National Laboratory [5]. Contudo, sua implementação ainda enfrenta desafios regulatórios, técnicos e sociais [6],[7].

Diante disso, o presente artigo tem como propósito a aplicação de um framework de gestão de riscos de cibersegurança voltado ao monitoramento remoto de SMRs no Brasil. Com o crescimento de pesquisas sobre o uso dessas tecnologias no país, surge a necessidade de um controle sobre sua operação, que envolve tanto questões físicas quanto cibernéticas. O framework foi baseado nas diretrizes do National Institute of Standards and Technology (NIST) [1], no NEI 08-09 [8], no Guia Regulatório 5.71 [9] e entre outros documentos para reatores SMRs [10-13].

2. METODOLOGIA

A expansão das ameaças à segurança cibernética está intrinsecamente ligada à crescente interconexão dos sistemas de infraestrutura crítica [14]. Isso acarreta riscos significativos para a estabilidade de um país, abrangendo áreas como segurança, economia, e até mesmo a saúde pública. A Fig. 1 dispõe o gráfico publicado pela International Energy Agency (IEA), no qual aponta uma média crescente de ataques cibernéticos ocorridos em diferentes setores nos anos de 2020 a 2022 [15].

Assim, a implementação de um Framework se torna essencial para quaisquer empresas ou organizações que queira gerenciar o uso do futuro reator SMR. Além disso, os procedimentos de gestão de riscos e o plano de segurança cibernética presentes no framework podem ser adaptados para incorporar melhorias, alinhando-se com as boas práticas predominantes do setor de interesse. Outra vantagem é que, para organizações que não possuem um programa de segurança cibernética preexistente, o framework pode ser utilizado como uma referência para a criação de um novo programa [15].

A determinação sobre como aplicá-lo é delegada à organização responsável pela implementação. Por exemplo, uma organização pode optar por adotar os Níveis de Implementação do Framework, para detalhar as práticas de gestão de riscos planejadas [15]. Em contraste, outra entidade pode utilizar as cinco Funções do Framework para avaliar integralmente seu conjunto de estratégias de gerenciamento de riscos. Essa avaliação de implementação pode ou não incorporar orientações suplementares de maior especificidade, como catálogos de controles [15][16].

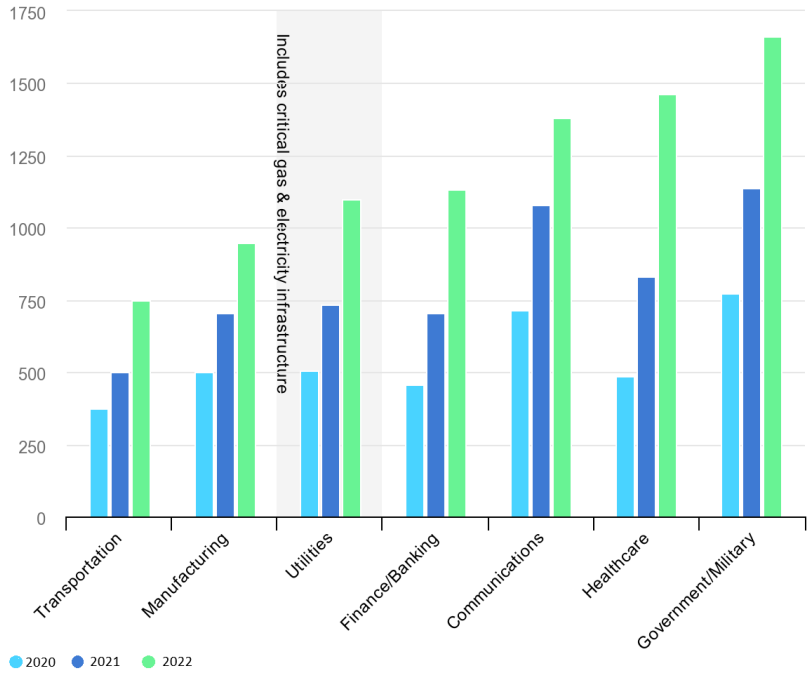

Fig. 1. Número médio de ataques cibernéticos semanais por organização em setores nos anos de 2020-2022 [14].

2.1 Construção do Framework

Para a construção do Framework foi utilizado como base as normas dos documentos NEI 08-09 [8], juntamente com o Guia Regulatório 5.71 [9]. Com isso, o Framework foi estruturado em etapas ou camadas, com o objetivo de fornecer uma abordagem integrada e abrangente para proteger os reatores SMR que podem ser controlados de maneira remota, contra ameaças cibernéticas. Dessa forma, para estruturar o framework foi necessário obedecer às funções do sistema que organizam as atividades básicas de segurança que são: identificar, proteger, detectar, responder e recuperar [15].

A função *identificar* estabelece o entendimento da organização sobre os riscos cibernéticos associados aos sistemas, pessoas, ativos, dados e capacidades dos SMRs. Já a função *proteger* tem ênfase no desenvolvimento e implementação de estratégias para garantir a continuidade dos serviços críticos de dados e informações. Quanto à função *detectar*, sua ênfase reside na concepção e execução de atividades adequadas para identificar prontamente a ocorrência de eventos de segurança cibernética. A função *responder*, por sua vez, é direcionada à ação imediata diante de um incidente, implementando medidas apropriadas em face de incidentes identificados. Já a função de *recuperar* compreende a manutenção dos planos de resiliência e a restauração de quaisquer recursos ou serviços que tenham sido afetados por incidentes de cibersegurança.

Para cada função foi estabelecido categorias ou subdivisões em grupos para descrever as atividades necessárias para o gerenciamento de riscos cibernéticos, levando em conta os riscos associados ao acesso remoto de SMRs. Posteriormente, para cada categoria, foi estabelecido subcategorias que especificam as atividades técnicas e/ou de gerenciamento. As subcategorias fornecem um conjunto de resultados que ajudam a apoiar a obtenção dos resultados em cada categoria, como está demonstrado na Fig. 2 através de um fluxograma.

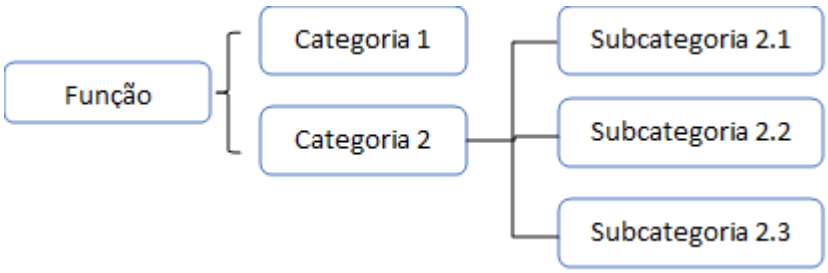

Fig. 2. Estrutura de construção do framework

Para melhor exemplificar, a Tab. 1 a seguir demonstra um bloco de estratégias pertencentes a função *Recuperar*, nas quais as subcategorias enumeradas como 2.1, 2.2 e 2.3 são pertencentes a categoria *Melhorias*. As subcategorias implementadas são a incorporação das lições aprendidas, estratégias de recuperação e atualização dos planos de identificação, proteção, detecção e resposta. Essas subcategorias são táticas e/ou atividades nas quais são conectadas intrinsecamente a esta classe.

Tab. 1: Práticas da função *recuperar* mapeadas para reatores SMR.

Função	**Categoria**	**Subcategoria**
Recuperar	1. Planejamento de Recuperação	1.1 O plano de recuperação é executado durante ou após um evento
	2. Melhorias	2.1 Os planos de recuperação incorporam as lições aprendidas
		2.2 As estratégias de recuperação são atualizadas
		2.3 Os planos de identificar, proteger, detectar e responder são atualizados
	3. Comunicações	3.1 As relações públicas são geridas
		3.2 Reputação após um evento ser reparado
		3.3 As atividades de recuperação são comunicadas às partes interessadas internas e às equipes executiva e de gestão

3. RESULTADOS

No desenvolvimento do framework para SMRs, foram implementadas subcategorias específicas para melhor adequação ao objetivo de gestão de riscos desses reatores. Na função *identificar*, foi criada uma subcategoria voltada para catalogar as plataformas de software e dispositivos de acesso remoto ao reator, além de mapear o fluxo de dados (Fig. 3). Essas ações visam identificar e compreender todos os elementos críticos, minimizando os riscos de ataques ao acesso remoto não autorizados e otimizando a supervisão dos dados. Ainda na função *identificar*, na categoria Estratégia de Gestão de Risco, foram adicionadas duas subcategorias associadas ao acesso remoto, como demonstra a Fig. 4.

Função	Categoria	Subcategoria
	1.Gestão de ativos	1.1 Catalogar plataformas de software e programas de acesso remoto do reator
		1.2 Catalogar dispositivos físicos e sistemas dentro da organização.
		1.3 Mapear a comunicação organizacional e os fluxos de dados.
		1.4 Recursos (por exemplo, hardware, dispositivos, dados e software) são priorizados com base em sua classificação, criticidade e valor comercial.

Fig. 3. Bloco de atividades da função Identificar, categoria indicada: 1. Gestão de ativos [17].

	5. Estratégia de Gestão de Risco	5.1 Os processos de gerenciamento de riscos são estabelecidos, gerenciados e acordados pelos envolvidos na organização.
		5.2 A tolerância a riscos organizacionais é determinada e expressa de forma clara.
		5.3 A determinação da tolerância a riscos da organização é informada pelo seu papel na infraestrutura crítica e pela análise de riscos específicos do setor.
		5.4 Identificar e adotar melhores práticas e padrões de segurança reconhecidos no setor
		5.5 Realizar uma avaliação abrangente dos riscos cibernéticos associados aos ativos de informações, considerando a probabilidade de ocorrência de ameaças e o potencial impacto dessas ameaças nos sistemas e dados da organização.

Fig. 4. Bloco de atividades da função Identificar, categoria indicada: 5. Estratégia de Gestão de Risco [17].

Essa categoria (Estratégia de Gestão de Risco) está relacionada as prioridades, restrições, tolerâncias de risco e suposições da organização que devem ser estabelecidas e usadas para apoiar as decisões de risco operacional. Dentro dessa categoria uma das subcategorias adicionadas foi a de "identificação de melhores práticas e padrões de segurança". Tendo esse enfoque consegue-se manter o direito individual dos colaboradores e mantem-se um equilíbrio entre segurança e liberdade no ambiente de trabalho. Foi pensado englobar neste tópico o treinamento de forma contínua dos colaboradores para a prevenção e remediação a ataques cibernéticos.

Foi reconhecido que, à medida que as ameaças cibernéticas se tornam mais sofisticadas, a resiliência de uma organização depende em grande parte da capacidade dos membros em identificar, responder e mitigar essas ameaças. Uma solução estratégica seria a construção de um aplicativo de treinamento dinâmico e contínuo, baseado em uma abordagem gamificada. O aplicativo teria como objetivo capacitar cada indivíduo a lidar com cenários de vulnerabilidade relacionados à cibersegurança de forma mais eficaz e engajadora.

A gamificação seria uma estratégia para proporcionar um ambiente de aprendizado envolvente, incentivando a participação ativa dos colaboradores e o desenvolvimento de habilidades práticas essenciais para a proteção dos reatores SMR. Acredita-se que essa abordagem, juntamente com a implementação do framework, não apenas fortaleceria a segurança cibernética desses sistemas críticos, mas também criará uma cultura de conscientização e responsabilidade em relação à cibersegurança.

Como prioridade de identificação, nesta categoria, também foi adicionado a realização de uma avaliação abrangente de riscos cibernéticos a reatores SMRs, considerando a probabilidade e o potencial de ocorrência de ameaças. Destaca-se que as avaliações sejam realizadas periodicamente em quaisquer empresas para a prevenção e detecção de ameaças futuras. A Fig. 5, apresenta parte do bloco da função *Detectar*, no qual, a categoria Segurança Contínua e Monitoramento, implementada para abordar o ambiente remoto de conectividade dos reatores modulares. As subcategorias 2.1 e 2.3 dispõe que a rede e todo ambiente remoto e as atividades das equipes devem ser monitoradas para detectar possíveis eventos de segurança cibernética [17].

Detectar	2. Segurança Contínua e Monitoramento	2.1 A rede e todo ambiente remoto são monitorados para detectar possíveis eventos de segurança cibernética
		2.2 O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética
		2.3 A atividade da equipe (presencial e remoto) é monitorada para detectar possíveis eventos de segurança cibernética
		2.4 Código malicioso é detectado
		2.5 Código móvel não autorizado é detectado
		2.6 A atividade do provedor de serviços externo é monitorada para detectar possíveis eventos de segurança cibernética
		2.7 O monitoramento de pessoal, conexões, dispositivos e software não autorizados é realizado
		2.8 As varreduras de vulnerabilidade são realizadas

Fig. 5. Bloco de atividades da função Detectar, categoria indicada: 2. Segurança Contínua e Monitoramento [17].

De forma concisa, para promover uma avaliação constante e aprimorar nosso sistema de segurança cibernética, foi incluído uma subcategoria na função *Recuperar* (Fig. 6). Essa subcategoria indica que após um incidente de ataque cibernético e a implementação das diretrizes deste framework, é essencial revisitar e atualizar o sistema. Essa abordagem tem o objetivo de se adaptar a novas ameaças e continuar progredindo para estar um passo à frente dos indivíduos por trás dos ataques.

Recuperar	2. Melhorias	2.1 Os planos de recuperação incorporam as lições aprendidas
		2.2 As estratégias de recuperação são atualizadas
		2.3 Os planos de identificar, proteger, detectar e responder são atualizados

Fig. 6. Bloco de atividades da função *recuperar*, categoria indicada: 2. Melhorias [17].

Assim, os blocos de funções do framework, voltado para a segurança de reatores nucleares SMR, tem por finalidade não apenas aprimorar a segurança do acesso remoto do reator, mas também estabelecer uma base sólida para a proteção contínua e aprimoramento do sistema de segurança cibernética, garantindo a capacidade de resposta a potenciais ameaças e a instalação e operação segura do reator. Este framework completo está disponível na referência Corrêa, Soares, Silva [17].

4. CONCLUSÃO

Durante o desenvolvimento deste estudo, o foco principal foi a criação de um framework de cibersegurança voltado para implementar ações em empresas ou organizações do Brasil que venham a operar reatores do tipo SMR. Foi considerado a crescente relevância desses sistemas no cenário energético global e a urgente necessidade de protegê-los contra ameaças cibernéticas em constante evolução. A criação do mencionado framework, pioneiro em nível nacional, foi identificada como um marco significativo na busca por soluções que assegurem a segurança e confiabilidade dos reatores SMRs, preenchendo uma lacuna nos estudos e abordagens relacionados à defesa cibernética desses sistemas. Embora este framework tenha sido desenvolvido com foco específico em reatores pequenos modulares, acredita-se que sua estrutura seja suficientemente robusta para ser adaptada a outros tipos de reatores nucleares e até mesmo em outros setores da indústria que lidam com infraestrutura crítica. No entanto, as particularidades dos SMRs, como a modularidade e o controle remoto, foram os principais motivadores para o desenvolvimento desta abordagem.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – PDPG-CONSOLIDACAO-3-4, o Conselho Brasileiro de Desenvolvimento Científico e Tecnológico - CNPq.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] FORCE, Joint Task, and Transformation Initiative. Security and privacy controls for federal information systems and organizations. **NIST Special Publication** 800.53 (2013): 8-13.

[2] LI, Ling et al. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. **International Journal of Information Management**, v. 45, p. 13-24, 2019.

[3] JARDINE, Cindy et al. Risk management frameworks for human health and environmental risks. **Journal of Toxicology and Environmental Health** Part B: Critical Reviews, v. 6, n. 6, p. 569-718, 2003.

[4] CALDER, Alan. **NIST Cybersecurity Framework: A pocket guide**. IT Governance Publishing Ltd, 2018.

[5] CHRISTENSEN, Jason et al. United States–Brazil Joint Study: A Preliminary Assessment of Opportunities and Challenges for Small Modular Reactors in Brazil. **INL/RPT-22-67191**, 2023.

[6] SOLER, Vaya, et al. Small Modular Reactors: Challenges and Opportunities (NEA-7560). **Nuclear Energy Agency of the OECD (NEA)**, 2021.

[7] Middleton, Bobby D. et al. Security by Design Economics Analysis for Advanced Reactors and Small Modular Reactors. **Project Interim Report for FY2021**. United States: N. p., 2021.

[8] NEI, J. NEI 08-09 Cyber Security Plan for Nuclear Power Reactors. **Nuclear Energy Institute**, 2010.

[9] POGACIC, Goran. Cyber Security in Nuclear Power Plants-US NRC. **Regulatory Guide 5.71**. 2014.

[10] LY, J. **Physical security for small modular reactors**. Disponível em: <https://www.nrc.gov/docs/ML1222/ML12221A197.pdf>. Acesso em: 6 set. 2023.

[11] EVANS, A. et al. **Physical Protection Recommendations for Small Modular Reactor Facilities**. Disponível em: <https://www.osti.gov/servlets/purl/1837151>. Acesso em: 6 set. 2023.

[12] INTERNATIONAL ATOMIC ENERGY AGENCY. **Governmental, Legal and Regulatory Framework for Safety General Safety Requirements Part 1: IAEA Safety Standards Series No. GSR Part 1**. International Atomic Energy Agency, 2010.

[13] US Nuclear Regulatory Commission. **Cyber security programs for nuclear facilities**. US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, 2010.

[14] PARKER, S.; WU, Z.; CHRISTOFIDES, P. D. Cybersecurity in process control, operations, and supply chain. **Computers & chemical engineering**, v. 171, n. 108169, p. 108169, 2023.

[15] AIE. **Cibersegurança – o sistema de energia está atrasado?**, AIE, Paris Disponível em: <https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind>, Licença: CC BY 4.0. Visto em 06 de set. de 2023.

[16] Cybersecurity & Infrastructure Security Agency (CISA). **Nuclear sector cybersecurity framework implementation guidance.** Disponível em: <https://www.cisa.gov/resources-tools/resources/nuclear-sector-cybersecurity-framework-implementation-guidance>. Acesso em: 6 set. 2023.

[17] Alberts, Christopher J.; Dorofee, Audrey J. **Risk Management Framework**. Software Engineering Institute, 2010.

[17] CORRÊA, K. M. S.; SOARES, J. B.; SILVA, C. F. T. Framework de Segurança Cibernética para Reatores Modulares Pequenos (SMR). Disponivel em: <https://office365ienmy.sharepoint.com/:f:/g/personal/guilherme_jaime_ien_gov_br/Es_ukMd5d0tOloqFLSRQz MMBihgbvkqGu8EQ00eu5WrY2A?e=6zPytg>. Acesso em: 05 Jul 2024.