Aplicação de rotinas operacionais de cibersegurança no setor de geração energia: desafios para o futuro

David C. P. da Cunha[1], **Milton Lima**[1], **Geraldo Cruz**[1]

[1]Instituto SENAI de Inovação para Tecnologia de Informação e Comunicação (ISI-TICs)
Av. Norte Miguel Arraes de Alencar, 539, 4º andar, Santo Amaro – Recife – PE – Brazil

{david.cunha}{milton.lima}{geraldo.cruz}@sistemafiepe.org.br

Abstract. *The power generation industry faces numerous cybersecurity threats. To mitigate the risk of attacks, power plants must adopt cybersecurity controls and routines in accordance with the National Electric System Operator (ONS). To this end, we propose in this work to identify challenges to the implementation of these operational routines in cybersecurity. The methodology included forms, a technical visit, and the generation of a report that can guide future implementations of operational routines in cybersecurity at ONS.*

Resumo. *O setor de geração de energia enfrenta inúmeras ameaças de segurança cibernética. Para mitigar riscos de ataques, as usinas de energia devem adotar controles e rotinas de cibersegurança conforme o Operador Nacional do Sistema Elétrico (ONS). Para esse fim, propomos neste trabalho, identificar desafios para a implantação desta rotinas operacionais em cibersegurança. A metodologia incluiu formulários, visita técnica e geração de relatório que podem nortear implantações futuras das rotinas operacionais em cibersegurança da ONS.*

1. Introdução

A infraestrutura energética de um país alimenta vários setores: indústria, governo, transporte, agricultura, água, redes de comunicação, ar, gás, iluminação pública e entretenimento. O setor de energia vem enfrentando crescentes ataques cibernéticos com impactos significativos, incluindo a interrupção do fornecimento [EPE 2023].

Atingir a cadeia de valor do setor com um ataque cibernético pode interromper os suprimentos, prejudicar a economia e até desestabilizar a segurança nacional. Implantar medidas de controle de cibersegurança pode enfrentar alguns desafios, visto que alguns sistemas de energia precisam reagir tão rápido que as medidas de segurança padrão, como a autenticação de um comando ou a verificação de uma assinatura digital, simplesmente não podem ser introduzidas devido ao atraso que essas medidas impõem [Sanders et al. 2022] [Das et al. 2020].

Outro ponto que deve ser observado e superado, se refere ao fato de que muitos elementos do sistema de energia foram projetados e construídos bem antes das considerações de segurança cibernética entrarem em ação. Esse legado agora precisa interagir com os mais recentes equipamentos de ponta para automação e controle, como medidores inteligentes ou aparelhos conectados e dispositivos de IoT (Internet das Coisas) sem ser exposto a ameaças cibernéticas [EPE 2023] [ONS 2022].

Com base no exposto, este artigo apresenta os desafios na implantação de rotinas de cibersegurança no setor de geração de energia. A metodologia incluiu entrevista com especialistas em cibersegurança do setor de geração de energia. Além disso, este trabalho apresenta ações para mitigar os desafios identificados nesta pesquisa.

2. Metodologia

A rotina operacional RO.CB.BR.01 do ONS (Operador Nacional do Sistema Elétrico) estabelece requisitos de segurança cibernética para o Sistema Interligado Nacional (SIN), que coordena a geração e transmissão de energia elétrica no Brasil. Seu objetivo é garantir a segurança operacional do SIN, protegendo contra possíveis ameaças e vulnerabilidades. O documento define requisitos e diretrizes para o planejamento, implementação e gestão da segurança cibernética [ONS 2022].

Entre os principais objetivos desta rotina podemos identificar: Identificar e avaliar os riscos cibernéticos; Estabelecer controles de segurança cibernética; Garantir a confidencialidade, integridade e disponibilidade das informações e sistemas; Estabelecer procedimentos para detectar, analisar e responder a incidentes de segurança cibernética; Estabelecer requisitos de treinamento e conscientização em segurança cibernética para os colaboradores envolvidos na operação; Garantir a conformidade com as leis, regulamentos e normas de segurança cibernética aplicáveis.

Para empresas de geração de energia elétrica, estar em conformidade com as rotinas do ONS é importante para proteger a infraestrutura crítica contra ameaças, além de promover a cultura de segurança e aumentar a confiança dos stakeholders. É fundamental que as empresas de geração de energia elétrica implementem medidas de segurança cibernética robustas para garantir a continuidade da operação. É necessário que a empresa adeque seus processos à rotina o mais rapidamente possível.

Para identificar os desafios quanto a implantação das rotinas operacionais, a Figura 1 apresenta a metodologia adotada.

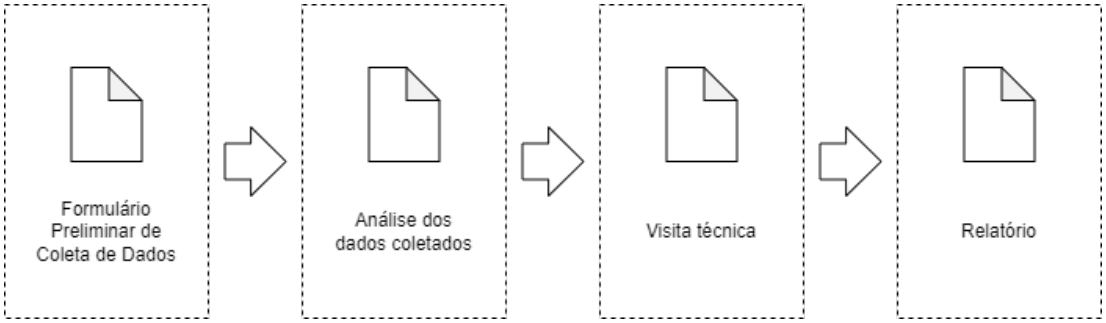

Figura 1. Metodologia

1. **Formulário preliminar de coleta de dados**. Foi criado um formulário contendo perguntas relacionadas aos requisitos da RO.CB.BR.01. O formulário [1] foi enviado por e-mail para facilitar o preenchimento e envio das respostas. Nesse momento preliminar, as perguntas foram mais abertas, deixando o respondente com mais liberdade para elaborar sua resposta, e permitindo uma avaliação mais qualitativa.

[1] acessível em `https://drive.google.com/file/d/1n9JYWHUpLWrmwIfgh5BGW1PZqxtErYsb/`

2. **Análise dos dados coletados**. As respostas do formulário foram analisadas para identificar possíveis dificuldades para implantar as rotinas operacionais.
3. **Visita técnica**. Foram realizadas visitas técnicas às usinas. Durante as visitas, foram entrevistados os responsáveis pela cibersegurança da empresa e os usuários do sistema de controle para levantar mais informações sobre as práticas de segurança.
4. **Relatório**. Foi elaborado um relatório técnico de avaliação da empresa, incluindo as informações coletadas, e os pontos relevantes com potencial para dificultar a implantação da rotina operacional. - O relatório foi encaminhado à equipe de cibersegurança da empresa, iniciando a discussão sobre as principais descobertas e recomendações.

3. Desafios

Durante o processo, foram avaliados aspectos relacionados aos requisitos de controle em cibersegurança especificados pelo ONS, como arquitetura tecnológica, governança de segurança da informação, inventário de ativos, gestão de vulnerabilidades, gestão de acessos e monitoramento de incidentes. A análise se concentrou em informações que pudessem impactar a cibersegurança local, considerando as diferenças estruturais entre as usinas e a criticidade da operação. No entanto, é importante ressaltar que a avaliação ficou restrita aos dados disponíveis nas observações, entrevistas e documentos analisados no período, com a participação dos especialistas disponíveis naquele momento.

A Figura 2 apresenta os principais desafios detectados para a implantação de rotinas de cibersegurança da ONS baseada no relatório.

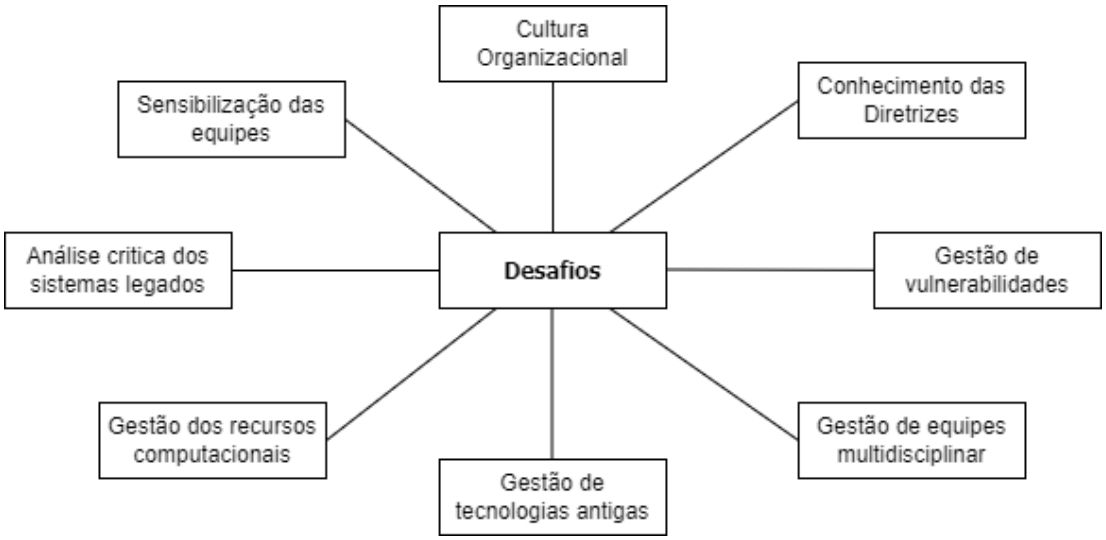

Figura 2. Desafios na Implantação de Rotinas operacionais da ONS

Implementar a segurança cibernética nas usinas é um desafio que envolve diversas questões culturais, técnicas e organizacionais. Um aspecto fundamental é compreender a cultura da empresa e garantir que ela esteja alinhada com a segurança cibernética. Para isso, é preciso conscientizar todas as pessoas da organização sobre as diretrizes de segurança da informação, estabelecidas por órgãos reguladores como a ANEEL e o ONS.

Além disso, é necessário definir mais claramente os papéis e responsabilidades relacionados à segurança cibernética na área de operação das usinas. Muitas vezes, exis-

tem muitos procedimentos internos voltados para a segurança das pessoas, mas falta uma tradução efetiva desses procedimentos em instrumentos normativos que possam ser seguidos e verificados de forma objetiva.

Outro desafio é lidar com a gestão de tecnologias antigas, que podem dificultar a implantação de controles e torná-los muito manuais. Sistemas críticos com décadas de uso provavelmente não foram projetados com a ciência dos requisitos de segurança atuais. É preciso implementar medidas de segurança para mitigar as vulnerabilidades desses sistemas e garantir que eles não representem ameaças para a organização.

Para isso, é importante que as vulnerabilidades sejam identificadas e corrigidas de maneira oportuna, considerando a complexidade dos sistemas. Isso requer a formação de equipes multidisciplinares, que envolvam profissionais de diferentes áreas, como engenharia, tecnologia da informação, segurança da informação e automação.

Por fim, é crucial gerenciar os recursos computacionais de maneira eficiente em sistemas críticos, garantindo a integridade, confidencialidade e disponibilidade dos dados. Com uma abordagem holística e colaborativa, é possível enfrentar os desafios da segurança cibernética nas usinas geradoras de energia e proteger os sistemas contra ameaças cibernéticas cada vez mais sofisticadas.

4. Conclusão

Este trabalho apresentou os principais desafios para a implantação de rotinas operacionais como a RO.CB.BR.01 no setor de geração de energia. Tendo como principal motivação a referida rotina operacional, foram realizadas entrevistas com especialistas em cibersegurança para identificar estes desafios, bem como a oportunidade de melhorar a proteção das estruturas críticas contra incidentes de segurança cibernética, em consonância com outras normas e padrões internacionais, como o NIST[NIST 2013]. Nesta pesquisa, foi possível acessar a estrutura de um grupo com mais 15 usinas no Brasil.

Como trabalho futuro motivado por este estudo, uma pesquisa está sendo conduzida com o objetivo de desenvolver um framework que apoie a implantação das rotinas operacionais do setor de geração de energia. O framework visará possibilitar a realização ágil de avaliações de maturidade e identificação dos riscos associados ao setor.

Referências

Das, L., Munikoti, S., Natarajan, B., and Srinivasan, B. (2020). Measuring smart grid resilience: Methods, challenges and opportunities. *Renewable and Sustainable Energy Reviews*, 130:109918.

EPE (2023). Empresa de pesquisa energética, anuário estatístico de energia elétrica 2022.

NIST (2013). Security and privacy controls for federal information systems and organizations. Technical Report NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015, National Institute of Standards and Technology, Gaithersburg, MD.

ONS (2022). Operador nacional do sistema elétrico divulga rotina operacional sobre segurança cibernética.

Sanders, P., Bronk, C., and Bazilian, M. D. (2022). Critical energy infrastructure and the evolution of cybersecurity. *Electricity Journal*, 35.