risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 30/10/2021
Aceitação/Acceptance: 20/01/2022

Avaliação da Rotina Operacional do Operador Nacional do Sistema Elétrico Brasileiro (ONS) em Relação às Ações de Gerenciamento de Riscos Associados à Segurança Cibernética

Eduardo De Oliveira Lima[1], Fernando Rocha Moreira[1], Flávio Elias Gomes de Deus[1], Georges Daniel Amvame Nze[1], Rafael Timóteo de Sousa Júnior[1], Rafael Rabelo Nunes[1,2,3]

oliveira-eduardo.eo@aluno.unb.br; fernando.moreira@aluno.unb.br; flavioelias@unb.br; georges@unb.br; desousa@unb.br; rafaelrabelo@unb.br

[1] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Engenharia Elétrica, CEP 70910-900 Brasília-DF Brasil

[2] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Administração, CEP 70910-900 Brasília-DF Brasil

[3] Centro Universitário Atenas, Rua Euridamas Avelino de Barros, nº 1400, Prado, CEP 38602-002 Paracatu-MG Brasil

Pages: 301-312

Resumo: Este trabalho tem por objetivo comparar os controles mínimos de segurança cibernética definidos pelo Operador Nacional do Sistema Elétrico Brasileiro (ONS) com aqueles recomendados pelo Center for Internet Security (CIS) para avaliar se a Rotina Operacional do ONS inclui controles suficientes para lidar com os riscos cibernéticos do setor elétrico. Foi utilizada uma escala de cinco níveis contidas no CIS CSC para realizar a comparação. Os resultados mostram que um dos dezoito grupos de controle que o ONS recomenda excede as exigências do Framework. Em contraponto, cinco outros grupos de controle não são mencionados pelas recomendações do ONS, e, para os outros grupos, os requisitos do ONS ficam aquém da estrutura do CIS CSC. Este trabalho contribui para o debate de risco cibernético relacionado à infraestrutura operacional do Sistema Elétrico Brasileiro (SEB), que, de acordo com os resultados, ainda necessita de melhorias em sua maturidade de gestão e operacional.

Palavras-chave: CIS CSC, Segurança Cibernética, Setor Elétrico, ONS, Gestão de Riscos

Assessment of the Brazilian National Electrical System Operator (ONS) Operational Routine regarding actions to manage the cybersecurity risks

Abstract: This paper aims to compare the minimum cybersecurity controls set by the Brazilian National Electric System Operator (ONS) with those recommended

by the 'includes sufficient controls to address cyber risks in the electricity sector. The Scale used in the CIS CSC contain five-level to perform the comparison. The results show that one of the eighteen control groups that ONS recommends exceeds the requirements of the Framework. In contrast, the ONS recommendation did not mention five other control groups, and for the other groups, the ONS requirements fall short of the CIS CSC Framework. This work contributes to the cyber risk debate related to the operational infrastructure of the Brazilian Electric System (SEB), which, according to the results, still needs improvements in its management and operational maturity.

Keywords: *CIS CSC, Cybersecurity, Electric Field Supplier Sector, ONS, Risk Management*

1. Introdução

As vulnerabilidades cibernéticas dos Sistemas de Controle Industrial (ICS) têm sido alvos de constante e crescente interesse de grupos *hackers*. Por exemplo, em 2010, o *malware Stuxnet* causou danos significativos ao Sistema de Supervisão e Aquisição de Dados (SCADA) das centrífugas no Irã (Baezner et al, 2017). Nos anos seguintes, vários casos também foram relatados: em 2014, a campanha de ataque *Havex* (Pixel, 2014) e a campanha *Sandworm* usando uma vulnerabilidade de dia zero para atingir o sistema SCADA da *General Electric* (GE) (Muncaster, 2014), e nos anos de 2015 a 2017, as ações destrutivas do *malware* Killdisk (Zetter, 2016) e Industroyer (Greenberg, 2017) causaram o desligamento da rede elétrica ucraniana. Eventos como estes levaram o Departamento de Segurança Nacional dos EUA (DHS) e o *Federal Bureau of Investigation* (FBI) a emitir um alerta em 2018 sobre ataques direcionados a energia e outros setores industriais críticos, quase todos eles direcionados aos sistemas de supervisão e aquisição de dados - SCADA (USCERT, 2018).

A este respeito, o ONS, considerando os riscos cibernéticos a que são submetidas as instalações do Sistema Elétrico de Potência - SEP, essencialmente aquelas sob influência do Sistema de Supervisão e Aquisição de Dados - SCADA, publicou em 09 de julho de 2021, uma Rotina Operacional (RO) que tem o objetivo de determinar aos agentes do Setor Elétrico Brasileiro - SEB a implantação de controles mínimos de segurança cibernética no Ambiente Regulamentado denominado ARCiber (ONS, 2021). Até o momento, não existem registros de outras rotinas operacionais do ONS, pertencentes ao Manual de Procedimentos Operacionais - MPO, que abordam a gestão da segurança cibernética no setor elétrico brasileiro.

O escopo do ARCiber é o ambiente operacional composto pelo conjunto de redes e equipamentos considerados no domínio da RO, a saber: os centros de operação dos agentes; os equipamentos participantes da infraestrutura de envio ou recebimento de dados e voz para os ambientes operacionais do ONS; os centros de operação de outros agentes; e, também, o ambiente operacional do ONS.

Neste contexto, surge uma pergunta: a implementação destes controles mínimos seria suficiente para enfrentar os riscos cibernéticos no setor elétrico? Como resposta, este trabalho se propôs avaliar a rotina publicada pelo ONS, e compará-la com a estrutura de segurança cibernética do CIS CSC V 8.0 (CIS, 2021).

A escolha do CIS CSC V 8.0 como parâmetro de comparação foi baseada no fato de ser ele um *Framework* otimizado, pois foi construído a partir de uma simplificação das estruturas NIST_SP_800_53 (NIST SP, 2020) e NIST_CSF (NIST CSF, 2018), que podem representar custos de implementação muito altos (DRTNS, 2016). Este *framework* selecionou os controles que oferecem a melhor relação risco/retorno em sua implementação. Com isto em mente, pretende-se avaliar se a proposta feita pela ONS é compatível com um padrão aceito como mínimo pela comunidade de segurança cibernética.

Este documento está organizado da seguinte forma: a Seção 2 abordará as referências teóricas, caracterizando o ambiente de estudo, tecnologias e padrões aplicáveis à segurança cibernética de infraestruturas críticas; a Seção 3 apresentará a metodologia adotada para o desenvolvimento do trabalho; a Seção 4 apresentará a análise dos resultados obtidos e uma breve discussão; e a Seção 5 mostrará as conclusões deste estudo.

2. Referencial Teórico

O SEP consiste em um complexo sistema de engenharia no qual o centro de controle concentra a responsabilidade pelo monitoramento, controle e tomada de decisões operacionais em tempo real (Sridhar & Hahn, 2012). Além disso, os sistemas cibernéticos que consistem em dispositivos eletrônicos de campo, como vistos em redes de comunicação, sistemas de automação de subestações e centros de controle, são incorporados em toda a rede física e envolvem os segmentos de geração, transmissão e distribuição de energia (Laprie et al, 2008). Assim, esta infraestrutura representa uma tecnologia muito diversificada com vários graus de conectividade. Além disso, como um desafio clássico, manter o equilíbrio dinâmico entre oferta e demanda de eletricidade é um aspecto fundamental que precisa ser mantido e garantido em tempo real (Arghandeh et al, 2016).

Nos últimos anos, o uso de dispositivos eletrônicos inteligentes (IEDs) tem sido disseminado para enfrentar estes desafios. Estes dispositivos permitem o gerenciamento do equilíbrio energético, uma vez que operam sistemas de proteção, supervisão, comando e controle do sistema elétrico (Huang et al, 2009). Entretanto, o intercâmbio de dados realizado por estes componentes tem como consequência o aumento das vulnerabilidades da superfície de exploração nos IEDs (Laprie et al, 2008) (Arghandeh et al, 2016). Os sistemas elétricos de comando e controle de potência são compostos por uma série de laços responsáveis pela identificação dos sinais de comunicação, protocolos, máquinas/dispositivos, processamento e ações de controle, associados a cada classificação funcional. Os impactos potenciais dos ataques cibernéticos estão concentrados principalmente nestes processos (Huang et al, 2009).

Os processos de avaliação dos riscos cibernéticos, associados à segurança das redes de energia elétrica, devem ser continuamente reavaliados, visando garantir uma operação com um nível adequado de segurança (Parks, 2007). Entretanto, a complexidade do SEP, a longa vida útil de seus componentes e a constante evolução das ameaças cibernéticas começaram a apresentar um novo vetor de ataque. A detecção e remoção dos problemas de segurança cibernética começaram a indicar a necessidade de abordagens específicas,

tanto para os sistemas e aplicações de energia (SPCS) como também para os sistemas e aplicações associados ao suporte da infraestrutura de Tecnologia da Informação (TI) (Permann & Rohde, 2005). Considerando o cenário de riscos cibernéticos apresentado para o SEP, entende-se que é de grande importância tratar a questão a partir de uma abordagem de gerenciamento de risco. Neste sentido, o apoio às normas e diretrizes de segurança, difundidas e aceitas pela comunidade internacional, torna-se um fator de grande importância. Portanto, o desafio é definir um bom instrumento para gerenciar redes de energia elétrica, considerando a melhor relação risco/retorno para o ambiente cibernético.

2.1. Padrões clássicos para o gerenciamento da segurança cibernética

O Guia de Segurança Cibernética das Redes Elétricas Inteligentes, NISTIR-7628 (US Department of Commerce, 2014), publicado pelo *National Institute of Standards and Technology* (NIST), propôs um conjunto de requisitos de segurança cibernética abrangente para garantir a adequação do mecanismo de proteção cibernética. Portanto, trata-se de um guia de grande importância para os sistemas que integram a infraestrutura de processos críticos, tais como os Sistemas Elétricos de Potência.

Devido a sua evolução, o NIST publicou as estruturas NIST_SP_800_53 e NIST_CSF, que apresentam uma vasta lista de controles que precisam ser gerenciados para garantir um nível adequado de segurança cibernética para as interfaces do SEP identificadas.

Além das estruturas publicadas pelo NIST, a Organização Internacional de Normalização (ISO) disponibilizou normas para a segurança da informação e gerenciamento de riscos, entre as quais a série ISO/IEC 27000 (ISO, 2022) e a série ISO/IEC 31000 (ISO, 2018), respectivamente, podem ser destacadas.

Entretanto, o NIST procurou harmonizar as normas internacionais e americanas, possibilitando um sistema de gerenciamento de segurança da informação e um processo de gerenciamento de risco baseado nas melhores práticas das normas ISO/IEC e COBIT 5 (ISACA, 2013). Portanto, o *Council on Cybersecurity* (CCS) *Top 20 Critical Security Controls* (CSC), ANSI/ISA-62443-2-1 (ISA, 2009), e ANSI/ISA-62443-3-3 (ISA, 2013) fornecem uma forma de facilitar a conformidade com base nas normas internacionais, bem como nas normas e diretrizes do NIST.

2.2. Controles do CIS CSC Versão 8

O padrão proposto pela NIST para a gestão da segurança cibernética é bastante abrangente, consistindo em cinco funções que incluem vinte e três categorias e cento e oito controles (subcategorias). O NIST reforça a tendência de custos elevados para sua implementação completa (DRTNS, 2016).

Este aspecto motivou o CIS a construir uma estrutura mais otimizada, consistindo em dezoito grupos de controles obtidos a partir do CSF da NIST. Estes controles destinam-se a atender às exigências das infraestruturas críticas com a melhor relação risco/retorno, com base no Princípio de Pareto, que define que 20% das causas são responsáveis por cerca de 80% dos efeitos, portanto, cerca de 20% dos controles do NIST podem representar 80% de melhoria no nível de segurança cibernética (McClain & Sagerand, 2018)

Além disso, os controles são estruturados em Grupos de Implementação (IGs), que consideram os recursos e o perfil de risco de cada organização. Assim, a implementação dos controles do CIS CSC começa com o grupo IG1, que é obrigatório para todas as organizações (incluindo aquelas com recursos limitados), seguido pelo grupo IG2, que considera organizações com recursos moderados, e finalmente, o grupo IG3, para organizações com exposição a alto risco. Portanto, o número de controles do IG3 é maior que o IG2, e o IG2 é maior que o IG1, como mostra a Tabela 1, a seguir.

Observe que os grupos 13, 16 e 18 não têm controles IG1, mas IG2 e IG3. Portanto, estes controles são implementados em organizações com maior disponibilidade de recursos.

Grupos de Controles CIS CSC	IG1	IG2	IG3
1- Inventário e Controle de Dispositivos de *Hardware*	2	4	5
2- Inventário e Controle de Ativos de *Software*	3	6	7
3- Proteção de Dados	6	12	14
4- Configuração Segura dos Softwares e Ativos Empresariais	7	11	12
5- Grenciamento de Contas	4	6	6
6- Gerenciamento do Controle de Acesso	5	7	8
7- Gerenciamento Contínuo de Vulnerabilidades	4	7	7
8- Gerenciamento dos Logs de Auditoria	3	11	12
9- Proteção de *e-mails* e Navegadores WEB	2	6	7
10- Proteção contra aplicações maliciosas	3	7	7
11- Recuperação de Dados	4	5	5
12- Gerenciamento da Infraestrutura de Rede	1	7	8
13- Defesa e monitoramento da Rede	0	6	11
14- Treinamento de Conscientização e Habilidades de Segurança	8	9	9
15- Gerenciamento de Provedor de Serviços	1	4	7
16- Segurança de Softwares e Aplicativos	0	11	14
17- Gerenciamento de Resposta a Incidentes	3	8	9
18- Teste de Penetração	0	3	5

Tabela 1 – Grupos de controle do CIS CSC e o número de subcontroles (salvaguardas) em cada grupo de implementação

2.3. Rotina Operacional do ONS

Em 09 de julho de 2021, o ONS, entidade responsável pela coordenação e controle das instalações de geração e operação de transmissão de eletricidade no Sistema Interligado Nacional - SIN, emitiu o RO-CB.BR.01 R00, pertencente ao Módulo 5 - Submódulo 5.13 do Manual de Procedimentos Operacionais - MPO, com o objetivo de orientar os Agentes do Setor Elétrico a adotarem controles mínimos de Segurança Cibernética para o Ambiente Regulamentado de Segurança Cibernética (ARCiber).

A Tabela 2 mostra os Grupos de Segurança definidos na Rotina Operacional (RO) e seus níveis de proteção. Os Agentes do Setor Elétrico Brasileiro devem direcionar seus esforços de controle e gestão, visando o cumprimento da RO em vinte e sete meses, após a publicação da norma, ou seja, em setembro de 2023.

Grupo de Segurança ARCiber	Macro Controles ARCiber
1- Arquitetura Tecnológica para o Ambiente do ARCiber	Redes Segregadas ARCiber isolado da Internet Existência de soluções *anti-malware* implantadas e atualizadas no ARCiber
2- Governança de Segurança da Informação	Existência de Processo Formal de Gestão da Segurança Cibernética no ARCiber
3- Inventários de Ativos	Realização de Inventário físico periódico de ativos de *hardware*, *software* e Dados conectados ao ARCiber Armazenamento Seguro do Inventário Físico
4- Gestão de Vulnerabilidades	Gestão da Implantação de Pacotes de Correção de Segurança Conexão de Novos Ativos ao ARCiber
5- Gestão de Acessos	Política de Gestão de Identidade e Acesso
6- Monitoramento e Resposta a Incidentes	Política de Monitoramento Plano de Resposta a Incidentes
7- Exceções	Tratamento de Exceções

Tabela 2 – Processo de Segurança Cibernética para o ARCiber (RO-CB.BR.01)

3. Metodologia

O presente trabalho representa uma pesquisa aplicada com objetivos exploratórios que teve como principal característica a captação de informações visando o entendimento de uma realidade, utilizando-se de investigações realizadas no contexto da pesquisa (Vergara, 2006). Trata-se de um trabalho qualitativo, uma vez que se valeu da análise de material documental como um dos principais métodos adotados (Prodanov & Freitas, 2013).

Para responder à pergunta proposta no objetivo deste trabalho, ou seja: "A Rotina Operacional do ONS é suficiente para lidar com os riscos cibernéticos do setor elétrico?", comparamos os controles da Rotina Operacional RO-CB.BR.o com os controles estruturais do CIS CSC. Dessa forma, os resultados obtidos são considerados secundários, cuja pesquisa associada está correlacionada a diversas fontes de documentos como livros, normas, padrões, revistas, periódicos, revisões sistemáticas da literatura (Marconi, 2003).

A avaliação da relação entre os pares de controle CIS CSC e ARCiber considerou a intensidade da semelhança ou diferença entre os controles existentes em ambos, avaliando a relação da esquerda para a direita, ou seja, partindo da relação dos controles da estrutura CIS CSC para os itens de segurança propostos pelo ONS para o ARCiber.

Esta comparação utilizou os mesmos critérios de classificação que a estrutura do CIS CSC utiliza para se comparar com outras estruturas (CIS, 2021). A Tabela 3 mostrada a seguir apresenta estes critérios, destacando as avaliações qualitativas graduadas em cinco níveis: *Equivalent; Superset; Subset; Intersection; e None*.

Relação CIS x ARCiber	Atenuação Defensiva
Equivalent	O controle CIS contém o mesmo conceito de Segurança Cibernética do controle ARCiber.
Superset	O Controle CIS possui um conceito mais amplo de Segurança Cibernética e contém o controle ARCiber.
Subset	O Controle CIS possui um conceito mais restrito de Segurança Cibernética e está contido no controle ARCiber.
Intersections	Há muitas semelhanças entre os dois, porém nenhum dos dois está contido dentro do outro. Não pode ser usado para atender aos requisitos do outro.
None	Não há nenhum controle ARCiber que se relacione com o Controle do *framework* CIS.

Tabela 3 – Relação entre os controles CIS CSC e os controles ARCiber

Assim, considerando cada Grupo de Implementação IG, os dezoito macrocontroles CIS CSC, e seus respectivos subcontroles (salvaguardas) foram realizadas as comparações com os controles definidos no ambiente regulado ARCiber. Esta análise permitiu a construção de um mapeamento que mostra os 18 grupos de controle CIS CSC e como o ambiente regulado ARCiber se relaciona com cada Grupo de Implementação IG1, IG2 e IG3, de acordo com a classificação qualitativa exposta acima.

4. Resultados e Discussão

A Tabela 4 mostra os resultados da comparação realizada. Nos resultados, é possível observar que dos 18 grupos de controle do CIS CSC, apenas o grupo 9 do CIS CSC é um *subset* dos controles ARCiber, ou seja, o *framework* ARCiber é mais restritivo nesse grupo de controles. Isso é explicado por dois motivos: alguns dos controles não se aplicam ao cenário do ARCiber, e em outros, há superação das exigências do CIS CSC visto que o ARCiber determina a segregação absoluta da arquitetura da rede de operação e a corporativa, vedando acesso à internet pelos dispositivos IEDs.

CIS CSC x ARCiber				Grupos de Controle ARCiber
Grupo CIS CSC	**IG1**	**IG2**	**IG3**	
1	*Equivalent*	*Superset / None*	*None*	*Groups 3 e 6*
2	*Equivalent*	*Superset / None*	*None*	*Groups 3 e 6*
3	*None*	*None*	*None*	-
4	*Equivalent / None*	*None*	*None*	*Groups 1, 3, 4, 5 e 6*

CIS CSC x ARCiber				**Grupos de Controle ARCiber**
Grupo CIS CSC	**IG1**	**IG2**	**IG3**	
5	*Equivalent / Superset*	*None*	*None*	*Groups 3 e 5*
6	*Equivalent / Superset*	*None*	*None*	*Groups 3 e 5*
7	*Equivalent / Superset*	*None*	*None*	*Groups 3, 4 e 6*
8	*Equivalent*	*Equivalent / None*	*None*	*Groups 6*
9	*Subset*	*Subset*	*Equivalent*	*Groups 1*
10	*Equivalent*	*Equivalent / Superset*	*Equivalent / Superset*	*Groups 1*
11	*None*	*None*	*None*	-
12	*Equivalent*	*Equivalent / None*	*None*	*Groups 1, 3, 4 e 5*
13	-	*Equivalent*	*Equivalent*	-
14	*None*	*None*	*None*	-
15	*None*	*None*	*None*	-
16	-	*None*	*None*	-
17	*Equivalent*	*Equivalent*	*None*	*Groups 2 e 6*
18	-	*None*	*None*	-

Tabela 4 – Comparação entre os Controles do *Framework* CIS CSC x Controles ARCiber da Rotina Operacional RO-CB.BR.01, Rev. 00

No outro extremo, tem-se que 6 dos 18 grupos de controles do CIS não tem nenhuma menção no ARCiber em nenhum dos níveis de implementação IG1, IG2 e IG3. Nesses grupos há identificação de "None" nos resultados da Tabela 4. São eles: 3 (Proteção de dados), 11 (Recuperação de Dados), 14 (Treinamento de Conscientização e Habilidades de Segurança), 15 (Gerenciamento de Provedor de Serviços), 16 (Segurança de Softwares e Aplicativos) e 18 (Testes de penetração). Isso significa que a aplicação desses controles por agentes do setor elétrico pode ser considerada opcional. Apesar de a não aplicação de controles do Grupo 3 ser justificável, já que os agentes não tratarão dados pessoais em sua maioria, a não previsão de controles dos grupos 11, 14, 15, 16 e 18 demonstra um baixo nível de maturidade na segurança cibernética do setor elétrico brasileiro. Nesse quesito, é importante registrar dois pontos: a falta desses controles pode dificultar no sucesso na implantação de programas de segurança cibernética (Muflihah & Subriadi, 2018) (Al-Daeef et al, 2017)(Feng et al, 2019) (Thomas et al, 2018) (Khera et al, 2019) e ainda, potencializar o impacto de riscos que porventura comprometam os discos rígidos dos equipamentos, pois não se menciona em nenhum momento da RO, a obrigatoriedade de rotinas de backup e recuperação de dados (Grupo 11).

Quando se considera o grupo de implementação IG2, os grupos de controle 1, 2, 8, 10, 12, 13 e 17 possuem equivalência relativa, sendo que em alguns casos, os controles do CIS são mais abrangentes do que o do ARCiber. Além disso, registra-se que os grupos de controle 3, 4, 5, 6, 7, 11, 14, 15, 16 e 18 não tem correspondência com o ARCiber.

Considerando o grupo de implementação IG3, o ARCiber não possui equivalência com a maioria dos controles, tendo alguma relação apenas nos controles dos grupos 9, 10 e 13, o que expõe muitas lacunas quando se consideram os controles que deveriam ser aplicados em ambientes com alto risco e criticidade, que é o caso do SEB.

Esses resultados demostram que o nível de controle que será exigido para o ARCiber se aproxima mais ao do grupo de implantação IG1, que conforme descrito, se aplicaria às organizações com restrições de recursos, o que não deveria ser o caso.

5. Conclusões e Trabalhos Futuros

Esse trabalho teve como principal objetivo responder à pergunta: a RO-CB.BR.01 Rev. 00 do Operador Nacional do Sistema Elétrico é suficiente para enfrentar riscos cibernéticos no setor?

Para isso, o trabalho comparou a RO com o *framework* CIS CSC que é amplamente utilizado na área de segurança cibernética e já é uma simplificação de outros *frameworks*.

A comparação foi realizada utilizando avaliações qualitativas graduadas nos 18 grupos de controle, sendo que apenas um grupo de controle do ARCiber superou as exigências do *framework* CIS, se posicionando aquém nos demais. Dessa forma, chega-se a conclusão que a RO elenca um conjunto de controles significativamente menor do que os mínimos necessários para que os principais aspectos da segurança cibernética possam ser monitorados, gerenciados e tratados pelos Agentes do Setor Elétrico.

Considerando a criticidade do setor elétrico para o país e o volume de recursos destinado a ele, entende-se que o nível de maturidade exigido para os controles do ARCiber, quando se verifica apenas a RO-CB.BR.01 Rev. 00, ainda é muito baixo, o que demonstra que a situação não estará confortável mesmo se todos os controles previstos para os agentes do setor elétrico sejam implantados até o final de setembro de 2023.

Destaca-se a falta de menção no ARCiber a controles de Recuperação de Dados; de Treinamento de Conscientização e Habilidades de Segurança; de Gerenciamento de Provedor de Serviços; de Segurança de Softwares e Aplicativos; e de Testes de penetração, que podem ter impactos significativos no resultado da implantação do programa de segurança cibernética dentro do setor.

Uma limitação do trabalho foi o grau de subjetividade que foi exigido para escolher um dos cinco níveis ao se fazer a comparação. Apesar disso, entende-se que essa limitação não compromete o resultado geral do trabalho, deixando aberta a discussão sobre segurança cibernética no setor elétrico brasileiro.

Sugere-se como trabalhos futuros, que se acompanhe a implantação desses controles, e que se compare as ações realizadas no ARCiber, com outros *frameworks* que se julgarem pertinentes para se realizar avaliação de possíveis gaps que porventura possam existir.

Agradecimentos

O autor Eduardo de Oliveira Lima agradece o suporte da Universidade de Brasília, por meio do DPG, Edital 01/2022; da ENBPar – Empresa Brasileira de Participações em Energia Nuclear e Binacional S/A. O autor Rafael Rabelo Nunes agradece o suporte do Centro Universitário Atenas e da Universidade de Brasília, por meio do Edital DPI/DPG 02/2022. Os autores Flávio Elias Gomes de Deus, Fernando Rocha Moreira e Rafael Rabelo Nunes agradecem o suporte do Ministério da Justiça e Segurança Pública representado pela Diretoria de Tecnologia da Informação e Comunicação (TED DTIC/SE/MJSP 01/2019). O autor Fernando Rocha Moreira agradece o suporte da FAP/DF, por meio do Edital 07/2022. O autor Rafael Timóteo de Sousa Júnior agradece o apoio do CNPq outorgas 465741/2014-2 e 312180/2019-5, da Advocacia Geral da União outorga 697.935/2019, do Departamento Nacional de Auditoria do SUS outorga 23106.118410/2020-85, da Procuradoria Geral da Fazenda Nacional outorga 23106.148934/2019-67, e do Conselho Administrativo de Defesa Econômica outorga 08700.000047/2019-14. O autor Georges Daniel agradece o suporte do laboratório LATITUDE / UnB por meio da outorga 23106.099441/2016-43 SDN.

Referências

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). "Security Awareness Training: A Review," in World Congress on Engineering.

Arghandeh, R., Meier, A. V., Mehrmanesh, L. & Mili, L. (2016). "On the definition of cyber-physical resilience in power systems," vol. 58, pp. 1060-1069. https://doi.org/10.1016/j.rser.2015.12.193.

Baezner M., & Robin, P. (2017). "Stuxnet," *Cyber Defense Project (CDP) and Center for Security Studies (CSS)*.

CIS, Center for Internet Security. (2021). "CIS Controls v8 Mapping to NIST_CSF_06_11_21".

CIS, Center for Internet Security. (2021). "Simplified & Prioritized Cyber Defense Guidance – CIS Critical Security Controls - CSC, Version 8.0".

DRTNS, Dimentional Research and Tenable Network Security, (2016). "Trends in Security Framework Adoption – A Survey of it and security professionals".

Feng, N., Wang, M., Li, M., & Li, D. (2019). "Effect of Security Investment Strategy on the Business Value of Managed Security Service Providers," *Journal Electronic Commerce Research and Applications,* vol. 35. https://doi.org/10.1016/j.elerap.2019.100843.

Greenberg, A. (2017). "Crash Override: The Malware That Took Down a Power Grid".

Huang, Y. L. & Cardenas, A. A. & Amin, S. & Z. S. Lin & H.-Y. Tsai & Sastry, S. (2009). "Understanding the physical and economic consequences of attacks on control systems," *International Journal of Critical Infrastructure Protect,* p. 73–83. https://doi.org/10.1016/j.ijcip.2009.06.001.

ISA, International Society of Automation, (2009). "ANSI/ISA–62443-2- 1 (99.02.01)-Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program".

ISA, International Society of Automation, (2013). "ANSI/ISA-62443-3-3 (99.03.03) - Security for industrial automation and control systems Part 3-3: System security requirements and security levels".

ISACA, Information Systems Audit and Control Association, (2013). "Transforming Cybersecurity: Using COBIT 5".

ISO, International Organization for Standardization, (2022). "ISO/IEC 27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements".

ISO, International Organization for Standardization, (2018). "ISO/IEC 31000 - Risk Management".

Khera, Y., Kumar, D., Sujay & Garg, N. (2019). "Analysis and Impact of Vulnerability Assessment and Penetration Testing," in *International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (Com-IT-Con)*. https://doi.org/10.1109/COMITCon.2019.8862224.

Laprie, J. C., Kanoun, K. & Kaaniche, M. (2008). "Modelling interdependencies between the electricity and information infrastructures," *Computer Safety, Reliability, and Security,* pp. 54-67. https://doi.org/10.1007/978-3-540-75101-4_5.

Marconi, M. L. (2003). "E. F. da M. Científica", 5ª edição, Editora Atas S.A. São Paulo

McClain, S. & Sagerand, T. (2018). "Auditing, Assessing, Analyzing: A Prioritized Approach using the Pareto Principle".

Muflihah, Y. & Subriadi, A. P., (2018). "A Basic Element of IT Business Continuity Plan: Systematic Review," *Jurnal Informatika,* vol. 12, no. 1, pp. 17-23. https://doi.org;10.26555/JIFO.V12I1.A8370.

Muncaster, P. (2014). "Microsoft Zero Day Traced to Russian 'Sandworm' Hackers," *Infosecurity Magazine*.

NIST Special Publication (SP) 800-53, Revision 5, (2020). "Security and Privacy Controls for Federal Information Systems and Organizations".

NIST_CSF, Cybersecurity Framework, Version 1.1, (2018). "Framework for Improving Critical Infrastructure Cybersecurity".

ONS, Operador Nacional do Sistema Elétrico, (2021). "Manual de Procedimentos da Operação Módulo 5 - Submódulo 5.13, Número RO-CB.BR.01, Revisão 00, Item 4.1.11".

Parks, R. C. (2007). "BSAND2007-7328: Guide to critical infrastructure protection cyber vulnerability assessment," *Sandia National Laboratories*.

Permann, M. R. & Rohde, K. (2005). "Cyber Assessment Methods for SCADA Security," in *15th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference*.

Pixel, A. (2014). "HAVEX Targets Industrrial Control Systems," *Trend Micro Threat Encyclopedia*.

Prodanov C. C., & Freitas, E. C. D. (2013). "Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico", 2ª Edição. [S.l.]: Editora Feevale

Sridhar, S., Hahn, A. & Govindarasu, M. (2012). "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE,* vol. 100, pp. 210-224. https://doi.org/10.1109/JPROC.2011.2165269.

Thomas, T. W. & Tabassum, M. & Chu, B. & Lipford, H. (2018). "Security During Application Development: an Application Security Expert Perspective," University of North Carolina at Charlotte - Department of Software and Information Systems.

United States Computer Emergency Readiness Team, (2018). "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors".

US Department of Commerce, National Institute of Standards and Technology, (2014). "NISTIR 7628 Revision 1 - Guidelines for Smart Grid Cybersecurity".

Vergara, S. C. (2006). "Projetos e relatórios de pesquisa". São Paulo: Atlas.

Zetter, K. (2016). "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid".

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 12/10/2021
Aceitação/Acceptance: 07/01/2022

Gestão de Riscos Cibernéticos no Ambiente Operacional do Sistema Elétrico Brasileiro (ARCiber ONS): uma avaliação do processo de recuperação de dados pelo sistema SCADA

Eduardo de Oliveira Lima[1], Fernando Rocha Moreira[1], Carlos André de Melo Alves[2], Rafael Rabelo Nunes[1,2,3]

oliveira-eduardo.eo@aluno.unb.br; fernando.moreira@aluno.unb.br; carlosandre@unb.br; rafaelrabelo@unb.br

[1] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Engenharia Elétrica, CEP 70910-900 Brasília-DF Brasil

[2] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Administração, CEP 70910-900 Brasília-DF Brasil

[3] Centro Universitário Atenas, Rua Euridamas Avelino de Barros, nº 1400, Prado, CEP 38602-002 Paracatu-MG Brasil

Pages: 313-325

Resumo: Com o aumento dos ataques cibernéticos ao setor elétrico, cada vez torna-se mais relevante proteger esse setor de riscos cibernéticos, além de se tornar resiliente para recuperar o ambiente em caso de ataques catastróficos. Esse artigo tem como objetivo avaliar a abrangência dos procedimentos de backup e recuperação de dados do sistema SCADA, visando identificar sua conformidade com os controles do Framework CIS que versam sobre o assunto. Para isso, foi analisado um manual operacional do sistema utilizando técnicas de análise de conteúdo. Verificou-se que há conformidade dos aspectos tecnológicos com o framework CIS, apesar de não ser possível garantir que empresas do setor elétrico brasileiro executem as rotinas de recuperação de forma sistemática. A relevância desse trabalho está na possibilidade da construção de um debate acerca do tema, diante das recentes ações do ONS para enfrentar riscos cibernéticos.

Palavras-chave: Setor Elétrico; SCADA, Backup e Recuperação de Dados; CIS; ONS; Segurança Cibernética; Riscos Cibernéticos.

Cyber Risk Management in the Brazilian Electric System Operational Environment (ARCiber ONS): Data Recovery Process Assessment by the SCADA System

Abstract: With the increase in cyber-attacks on the electric sector, it is becoming increasingly important to protect this sector from cyber-risks, in addition to becoming resilient to recover the environment in case of catastrophic attacks. This article aims to evaluate the backup and data recovery comprehensiveness of SCADA

system procedures, in order to identify its compliance with the CIS Framework controls that address the subject. To this end, this work analyzed a system operational manual using content analysis techniques. The research verified that there is conformity of the technological aspects with the CIS framework, although it is not possible to guarantee that companies from the Brazilian electric power sector execute the recovery routines in a systematic way. The relevance of this work lies in the possibility of building a debate about the topic, given the ONS' recent actions to address cyber risks.

Keywords: Electric Sector; SCADA; Data Backup Recovery; CIS; ONS; Cybersecurity; Cyber Risks.

1. Introdução

Os ataques cibernéticos em Sistemas de Infraestruturas Críticas (Industrial Control Systems – ICS) têm sido de interesse constante e crescente de grupos de Hackers. Mais especificamente, ataques cibernéticos provocaram um aumento significativo de ocorrências de violações na segurança dos Sistemas de Supervisão e Aquisição de Dados (SCADA), aumentando em 11% entre os anos de 2017 e 2018 e um acréscimo de 67% se for levado em consideração o período considerado entre os anos de 2013 e 2018 (Accenture Security, 2019). A campanha Sandworm atingiu o sistema SCADA da GE causando diversos tipos de danos, onde utilizou-se de uma vulnerabilidade de zero-day (Muncaster, 2014). Eventos como esses levaram o Department of Homeland Security - DHS dos EUA e o Federal Bureau of Investigation - FBI a emitirem um alerta, em 2018, de ataques direcionados à energia e outros setores industriais críticos, quase todos direcionados aos Sistemas SCADA (USCERT, 2018).

De forma similar, no Brasil, o Operador Nacional do Sistema - ONS publicou em 09 de julho de 2021 uma Rotina Operacional - RO, a qual tem por finalidade determinar aos agentes do Setor Elétrico Brasileiro – SEB a implantação de controles mínimos de segurança cibernética no Ambiente Regulado Cibernético - ARCiber (ONS, 2021).

O ARCiber tem como abrangência o ambiente operacional constituido pelo conjunto de redes e equipamentos que estão considerados no escopo da RO, quais sejam: os centros de operação dos agentes; os equipamentos que participam da infraestrutura de envio ou recebimento de dados e voz para ambientes operacionais do ONS; ou para centros de operação de outros agentes; e, ainda, o próprio ambiente operativo do ONS.

Essa RO apresenta sete dimensões de controles de segurança cibernética: Arquitetura Tecnológica para o Ambiente do ARCiber; Governança de Segurança da Informação; Inventários de Ativos; Gestão de Vulnerabilidades; Gestão de Acessos; Monitoramento e Resposta a Incidentes; e Exceções.

Além de se protegerem preventivamente de ataques cibernéticos, um elemento fundamental com o qual as empresas do setor elétrico devem fomentar para o aumento de suas resiliências é a execução sistemática de um processo de *backup* e recuperação de dados. No entanto, verifica-se que muitas empresas desse segmento ainda não padronizaram suas métricas associadas ao processo de gestão de riscos cibernéticos, deixando de conhecer e gerenciar adequadamente os seus parâmetros operacionais, tornando ainda mais vital a presença de uma gestão de riscos que contemple o processo

de recuperação de dados de forma clara e controlada (Plèta, 2021). Outro fato que corrobora com isso é que a lista de controles da RO não faz menção sobre procedimentos específicos sobre a gestão de recuperação de dados do ambiente ARCiber (ONS, 2021).

Nesse sentido, coloca-se a seguinte questão: os manuais de operação dos sistemas SCADA já abrangem rotinas suficientes de forma que a previsão de controles para essa dimensão fosse prescindível de auditoria pelo ONS? Dessa forma, esse trabalho tem como objetivo avaliar a abrangência dos procedimentos de backup e recuperação de dados do sistema SCADA, visando identificar sua conformidade com os controles do Framework CIS que versam sobre o assunto. Dessa forma, será possível verificar a disponibilidade de controles previamente existentes para uso do processo de gestão de riscos cibernéticos o que poderia justificar a dispensa da inserção obrigatória no ambiente regulado ARCiber, definido pela Rotina Operacional.

Esse trabalho está organizado da seguinte forma: além desta introdução, na seção 2 serão abordadas referências teóricas, caracterizando o ambiente de estudo, tecnologias e normas aplicáveis à segurança cibernética de infraestruturas críticas; na Seção 3 será apresentada a metodologia adotada para o desenvolvimento do trabalho; na Seção 4 será apresentada a análise dos resultados obtidos e uma discussão sobre o tema abordado; e, na Seção 5, serão mostradas as conclusões do presente estudo.

2. Referencial Teórico

Nessa seção, serão descritos os principais tópicos para compreensão desse artigo. Na seção 2.1, são tratados os aspectos do processo de Gestão de Riscos cibernéticos em Sistemas Eletricos de Potências. Na seção 2.2, abordamos o *framework* CIS CSC V8. Na seção 2.3, detalhamos a Rotina Operacional publicada pelo Operador Nacional do Sistema elétrico brasileiro, e por fim, na seção 2.4, abordamos os sistemas SCADA e seus processos de *backup* e recuperação de dados.

2.1. O processo de Gestão de Riscos Cibernéticos em Sistemas Elétricos de Potência

O processo de gestão de riscos cibernéticos passa, inicialmente, pela análise de vulnerabilidades a que está submetida a infraestrutura de um sistema elétrico em geral. As vulnerabilidades associadas aos sistemas de supervisão e aquisição de dados (SCADA) são umas das mais importantes a serem avaliadas em um processo de gestão de riscos cibernéticos (Stouffer et al, 2015). Nesses ambientes, as principais vulnerabilidades podem ser identificadas nos produtos de terceiros e softwares embarcados, assim como aquelas encontradas em configurações e fragilidades associadas à rede de comunicação (DHS CSSP, 2011).

Após a identificação de vulnerabilidades e riscos cibernéticos, a etapa de análise de impacto deve ser realizada para determinar as possíveis consequências nos aplicativos suportados pela infraestrutura elétrica (Sridhar et al, 2012). As atividades subsequentes têm por objetivo mitigar e minimizar os níveis de risco inaceitáveis (Laprie et al, 2007).

O processo de gestão de riscos cibernéticos exige, então, a definição de procedimentos e controles que irão permitir não apenas o monitoramento da execução das ações de

segurança e de mitigação de riscos, como também o acompanhamento sistemático da rotina e dos respectivos controles associados.

No entanto, é importante destacar que a manutenção da disponibilidade, da confidencialidade e da integridade das informações associadas aos controles só é possível caso eles sejam suportados sob três dimensões: tecnologia, processos, e pessoas (Nakamura, 2007), considerando o contexto de um processo de gestão de riscos cibernéticos.

2.2. CIS CSC Critical Security Controls Version 8

Os Controles apresentados no framework CIS Critical Security Controls constituem um conjunto prioritário de ações (salvaguardas) recomendadas para a defesa cibernética, que oferecem formas específicas e acionáveis de se impedir e mitigar os ataques cibernéticos mais usuais contra sistemas e redes. Esse framework é gerenciado pelo Center for Internet Security – CIS, e seus controles foram aprimorados para acompanhar os sistemas e softwares modernos (nuvem, virtualização, mobilidade, terceirização, trabalho remoto, evolução das táticas de ataque, etc.) (CIS, 2021).

O CIS CSC (CIS, 2021) foi escolhido para este trabalho por ser um *framework* otimizado, constituído de dezoito Macrocontroles obtidos a partir do Framework NIST_CSF - Cyber Security Framework (NIST, 2018).

Este framework estrutura os controles por meio de uma classificação de Implementation Groups - IGs, que levam em consideração os recursos e perfis de risco de cada organização. Dessa forma, a implantação dos controles CIS CSC começam pelos controles IG1, que são obrigatórios a todas as organizações (inclusive as com recursos limitados); seguindo com a implantação dos controles IG2, onde se considera organizações com recursos moderados, e por fim, os controles IG3, para organizações com alta exposição a riscos (Ibrahim, 2021).

O Macrocontrole 11 trata especificamente dos aspectos sobre Recuperação de Dados do Framework CIS CSC e tem por objetivo disponibilizar condições para se estabelecer e manter práticas de recuperação de dados que sejam suficientes para garantir a recuperação dos ativos empresariais para uma situação igual àquela identificada antes do incidente, de forma confiável e segura.

Esse Macrocontrole 11 é composto de cinco subcontroles, cuja abrangência atende às funções de segurança associadas à recuperação e proteção dos dados. São eles:

- Subcontrole 11.1 – Tem como objetivo estabelecer e manter um processo de recuperação de dados. No processo, deve ser abordado o escopo das atividades de recuperação de dados, a priorização da recuperação e a segurança dos dados de backup. Revisar e atualizar a documentação anualmente, ou quando ocorrerem mudanças significativas na empresa que possam impactar este Subcontrole (Salvaguarda);
- Subcontrole 11.2 – Realizar backups automatizados de ativos empresariais no escopo. Executar backups semanalmente, ou com maior freqüência, com base na importância dos dados;
- Subcontrole 11.3 – Proteger os dados de recuperação com controles equivalentes aos dados originais. Dependendo dos requisitos, pode ser utilizada criptografia ou separação de dados;

- Subcontrole 11.4 – Estabelecer e manter uma instância isolada de dados de recuperação. Exemplos de implementações incluem versão controlando destinos de backup através de sistemas ou serviços off-line, em nuvem ou fora do local;
- Subcontrole 11.5 – Testar a recuperação do backup trimestralmente, ou mais freqüentemente, para uma amostragem dos ativos da empresa no escopo.

Esses subcontroles atingem as três categorias de IGs, independentemente dos recursos e do perfil de risco de cada organização, exceto o Subcontrole 11.5, para o qual o CIS dispensa a sua adoção para o Grupo de Implantação IG1 (CIS, 2021).

No entanto, para as empresas de geração, transmissão e distribuição de energia elétrica, todos os subcontroles (salvaguardas), são importantes: "Para essas empresas, os processos são dotados de uma elevada criticidade, em especial aqueles monitorados pelo Sistema SCADA. As avaliações de segurança devem ser incluídas como parte da governança de um sistema crítico e seu gerenciamento de segurança" (Alcaraz & Zeadally, 2015).

2.3. Rotina Operacional do ONS

Em 09 de julho de 2021 o ONS, órgão responsável pela coordenação e controle da operação das instalações de geração e transmissão de energia elétrica no Sistema Interligado Nacional – SIN, emitiu a RO-CB.BR.01 R0, pertencente ao MPO Módulo 5 – Submódulo 5.13, que teve como objetivo definir e orientar os Agentes do Setor Elétrico quanto aos controles mínimos de segurança cibernética a serem adotados para o Ambiente Regulado Cibernético, o qual passou a ser chamado de ARCiber (ONS, 2021).

A Tabela 1 consolida os Grupos de Segurança definidos na RO, assim como os seus respectivos níveis de proteção, para os quais os agentes do Setor Elétrico Brasileiro deverão direcionar seus esforços de gestão e controle, visando à constituição de um ambiente minimamente seguro para as instalações operacionais (ONS, 2021).

Por meio da Tabela 1 é possível perceber a ausência, dentre outros, de macrocontroles ARCiber associados ao Macrocontrole 11 do Framework CIS CSC – Recuperação de Dados, o qual deve ser considerado, segundo o CIS CSC, por todas as empresas que tenham por objetivo implantar um processo de gestão de riscos cibernéticos, independentemente do tamanho e capacidade financeira.

Grupo ARCiber	Subcontroles ARCiber
1 – Arquitetura tecnológica para o ambiente do ARCiber	Redes segregadas
	ARCiber isolado da internet
	Existência de soluções anti-malware implantadas e atualizadas no ARCiber
2 – Governança de segurança da informação	Existência de processo formal de gestão da segurança cibernética no ARCiber
3 – Inventários de ativos	Realização de inventário físico periódico de ativos de hardware, software e dados conectados ao ARCiber
	Armazenamento seguro do inventário físico

Grupo ARCiber	Subcontroles ARCiber
4 – Gestão de vulnerabilidades	Gestão da implantação de pacotes de correção da segurança
	Conexão de novos ativos ao ARCiber
5 – Gestão de acessos	Política de gestão de identidade e acesso
6 – Monitoramento e resposta a incidentes	Política de monitoramento
	Plano de resposta a incidentes
7 – Exceções	Tratamento de exceções

Fonte: os autores a partir do conteúdo da RO-CB.BR.01 Ro

Tabela 1 – Processo de Segurança Cibernética para o ARCiber (RO-CB.BR.01)

2.4. Sistemas SCADA e os seus processos de recuperação de dados

O Sistema SCADA tem uma função crucial para os processos industriais: é ele que assume a responsabilidade pelo acompanhamento e supervisão dos processos produtivos, cujo principal objetivo é garantir a sua correta execução, de conformidade com os padrões de projeto. Ele ainda oferece os subsídios para a atuação de sistemas auxiliares de proteção, comando e controle por exemplo.

Ele é projetado para que seja possível a implementação de configurações específicas para cada tipo de processo, armazenar dados e disponibilizar recursos para intervir manualmente ou automaticamente no processo, quando necessário. Além de atuar preponderantemente em processos industriais, o SCADA também tem sido muito utilizado em processos experimentais (Daneels,1999).

Além de coletar os dados, o SCADA, também chamado de sistema supervisório, permite ainda a visualização e supervisão dessas informações. Essa visualização normalmente são apresentadas de forma amigável em telas sinópticas, se valendo de gráficos de tendências, evolução histórica e sinalização de alarmes e falhas

A infraestrutura associada aos Sistemas SCADA é constituída de servidores, drivers de comunicação, sensores e atuadores conectados ao processo. Com isso é possível a sua atuação em tempo real (Daneels,1999).

Uma variedade de sistemas SCADA está em operação nas subestações transformadoras de energia elétrica, providos por vários fabricantes diferentes.

O Sistema SCADA da Siemens, WinCC V7.5 SP2 possui um grande número de funcionalidades associadas aos procedimentos de arquivamento de dados do processo, assim como de arquivos de usuários (SCADA, 2020).

Para a execução desse trabalho, foi utilizada uma versão moderna do sistema SCADA, com escopo de funcionalidades abrangentes, em especial aquelas associadas aos processos de Backup/Recovery. Buscou-se utilizar um sistema SCADA que apresentasse um bom nível de automação e com alta tecnologia embarcada (SCADA, 2020).

O SCADA da Siemens apresenta os principais grupos de funcionalidades associadas ao Backup/Recovery, quais sejam:

- Archiving Fast e Slow;
- Backup de Arquivos de Processo;
- Configurações Gerais de Origem e Destino de Arquivos de Processo e de Usuários;
- Configurações de Infraestrutura de Rede e Servidores de Backup/Recovery;
- Links de Conexão com Servidores de Backup/Recovery;
- LOG de Monitoramento;
- Criptografia.

A partir desses grupos de funcionalidades é de se esperar que os subsídios necessários para a construção, alimentação e monitoramento dos subcontroles definidos no Macrocontrole 11 do CIS CSC estejam disponíveis, independentemente dos Grupos de Implantação (IG1, IG2 e IG3) a que pertencem.

O processo de análise de conteúdo realizado permitiu a identificação das principais funcionalidades do Sistema SCADA da Siemens, associadas à recuperação de dados, conforme descrito a seguir:

- Archieving fast e slow de dados de processo;
- Backup de arquivos de processo;
- Sistemas redundantes
- Ativação do backup
- Definição de caminhos de rede para dados de processo;
- Idem para dados de usuários;
- Servidor de Backup;
- Desconexão de arquivos;
- Gravação e Recuperação de Dados;
- Backup específico;
- Arquivos de usuários;
- Redundância em arquivos de usuários;
- Backup manual dos arquivos de usuário.

3. Metodologia

O presente trabalho representa uma pesquisa aplicada com objetivos exploratórios que teve como principal característica a captação de informações visando o entendimento de uma realidade, utilizando-se de investigações realizadas no contexto da pesquisa (Vergara, 2006). Trata-se de um trabalho qualitativo, uma vez que se valeu da análise de material documental como um dos principais métodos adotados (Prodanov, 2013).

Para se atingir o objetivo desejado, foram analisados os Capítulos 7 e 8 do Manual do Sistema SCADA Siemens WinCC V7.5 SP2. Dessa forma, os resultados obtidos são considerados secundários. Resultados nessa natureza são obtidos quando a pesquisa associada está correlacionada a fontes diversas, isoladas ou associadas, tais como documentos, livros, normas, padrões, revistas, periódicos e revisões sistemáticas da literatura (Marconi, 2003).

Os dados secundários obtidos foram analisados utilizando as técnicas de análise de conteúdo (Bardin, 2011), cujos passos estão descritos a seguir:

- Pré-análise: onde são feitos a leitura flutuante; escolha dos documentos; reformulações de objetivos e hipóteses e a formulação de indicadores (Bardin, 2011);
- Construção das Categorias: na qual a descrição analítica contribui fortemente para o estudo detalhado e consistente. Esse processo deve basear-se nas hipóteses e nos referenciais teóricos adotados (Mozzato & Grzyboviski, 2011). Na definição dessas categorias é realizada a classificação, quando se realiza o desmembramento e posterior agrupamento ou reagrupamento das unidades de registro do texto. Assim, a repetição de palavras e/ou termos foi a estratégia adotada no processo de codificação para serem criadas as unidades de registro e, posteriormente, as categorias de análise usadas inicialmente (Bardin, 2011);
- Tratamento dos resultados, inferências e interpretações: nesse momento devem ser realizadas as reflexões e críticas, as quais devem ser capazes de viabilizar os conteúdos de interesse existentes no material identificado, utilizando-se as ferramentas disponibilizadas durante o processo de análise de conteúdo. Trata-se de uma fase lógica, cujos resultados são obtidos a partir da conexões existentes entre proposições inferidas e outras já tidas como verdadeiras (Fossá, 2003).

Desse modo, foram realizadas as análises dos resultados obtidos a partir da comparação entre os Macrocontrole No. 11 do Framework CIS CSC e o ambiente regulado ARCiber definido pela RO do ONS.

4. Resultados

A Tabela 2 apresenta o número de ocorrências de palavras/termos de interesse nos Capítulos 7 e 8 do manual SCADA, obtidas por meio do software *Word Counter (*Countwordsfree*,* 2022*)*. Essa estratégia foi a adotada no processo de codificação para criar as unidades de registro (Bardin, 2011). Com isso, foram obtidas as unidades de registro mais representativas para a análise de conteúdo. Pelo resultado, verifica-se que o Sistema SCADA apresenta, em ordem decrescente, os termos 'Configuração', 'Arquivamento', 'Backup', 'Exportar dados', 'Importar', 'Gravar', 'Redundância', 'Restaurar', 'Recuperar'. Isso permite inferir que o foco principal do processo de Recuperação de Dados para o Sistema SCADA baseia-se em primeiro lugar na Configuração do Sistema, já que como pode ser observado, o número de ocorrências desse termo é quase o dobro do segundo. Em seguida, aparecem aspectos associados ao 'Backup', 'Exportação' e 'Importação' de Dados.

Por meio das unidades de registro apresentadas na Tabela 3, foi possível a definição das categorias iniciais. A Tabela 3 a seguir mostra a distribuição dessas categorias, baseando-se na significância das palavras e termos oriundos da leitura dos documentos.

Unidades de Registro	Número de ocorrências das Palavras
Configuração	641
Arquivamento	315
Backup	57
Exportar dados	34
Importar	22

Unidades de Registro	Número de ocorrências das Palavras
Gravar	13
Redundância	13
Restaurar	10
Recuperar	1

Fonte: os autores a partir de dados da pesquisa

Tabela 2 – Unidades de registro da documentação

Número	Categorias iniciais
1	Exportar registro de dados para backup de segurança
2	Arquivamento de valores de processo
3	Arquivamento de registros de usuários e configurações
4	Backup de valores de processo
5	Backup de registros de usuário
6	Recuperar e importar dados de processo para base de produção
7	Recuperar dados de configuração do SCADA
8	Recuperar dados do usuário
9	Ciclo de arquivamento em runtime
10	Configurações de arquivamento de valores de processo “archiving”
11	Arquivamento sob demanda
12	Arquivamento em Inicialização e desligamento do sistema
13	Ciclo de arquivamento processo ciclico e aciclico
14	Armazenamento de dados em memória

Fonte: os autores a partir de dados da pesquisa

Tabela 3 – Categorias iniciais

As categorias inciais, apresentadas na Tabela 3, foram definidas a partir das unidades de registro. Nesse sentido, tanto o Sistema SCADA, como a RO do ONS, sugeriram segmentos de atividades classificados pela sua importância no processo.

A partir das categorias iniciais, descritas na Tabela 4, foram definidas três categorias intermediárias, todas associadas ao objeto do Macrocontrole No. 11 do CIS CSC. Essas categorias intermediárias representam, respectivamente, um processo interno e externo de geração de backups, a geração dos arquivos internos de *runtime*, a partir dos quais os backups são gerados e, por último, o processo de recuperação de dados de processo e de usuários existentes em backup. Pelo exposto, é possível verificar que para os Subcontroles do Macrocontrole 11 do Framework CIS CSC, os subsídios para a sua efetiva construção e gerenciamento de recuperação de dados podem ser identificados no sistema SCADA, independentemente de o agente definir e operar um processo formal e estruturado de

backup e restauração de dados, que esteja vinculado a um processo de gestão de riscos. A Tabela 4 a seguir ilustra as categorias intermediárias identificadas e seus respectivos conceitos norteadores.

Categoria Intermediária	Conceito Norteador	Categoria Inicial
Geração de Backup externo ao SCADA **Atende: CIS CSC 11.1 e 11.4**	O Sistema SCADA é dotado de ferramentas responsáveis pela geração de cópias de arquivos de segurança externos ao runtime, os quais são armazenados em diretórios específicos informados por caminho a ser utilizado, podendo ser em Servidores da Rede de Comunicação de Dados ou armazenamento externo. Além da possibilidade de alta disponibilidade oferecida por um sistema com redundância (Cluster), o sistema também oferece outra via de recuperação de dados de processos e geração de backup, os quais são configurados no runtime ou gerados a partir de procedimentos manuais de exportação para arquivos externos.	[1][2][3]
Geração de arquivos internos ao SCADA com dados de processo e de usuários **Atende: CIS CSC 11.2**	Para a geração de backups de segurança, o sistema SCADA é configurado para a geração de arquivos em tempo real de informações do processo supervisionado ou arquivos de usuários que são utilizados para interfaces com sistemas de proteção, comando e controle, assim como informações de interface com plataformas externas. A geração das informações de processos obedecem configurações específicas que definem os ciclos a serem utilizados automaticamente ou arquivamento por demanda operacional e local de armazenamento.	[4][5][9][10] [11][12][13] [14]
Recuperação de arquivos Backup externo ao SCADA **Atende: CIS CSC 11.3 e 11.5**	A recuperação de dados armazenados em arquivos externos (backups) também é uma função customizável do Sistema SCADA e é realizada por comando interno manual configurável. Essa operação pode ser realizada por meio do método de recuperação do WinCC ou ação de importação, de forma segura e integra, utilizando arquivos gerados pelos métodos de backup internos (runtime em arquivos de processo e arquivos de usuário) ou externos (exportação), respectivamente.	[6][7][8]

Fonte: os autores a partir de dados da pesquisa

Tabela 4 – Categorias intermediárias

A partir das informações obtidas e organizadas nas Tabelas 2, 3 e 4 pôde-se verificar que os subsídios necessários para a geração dos controles previstos no Macrocontrole 11 do CIS CSC estão disponíveis, qualquer que seja o Grupo de Implantação (IG1, IG2 e IG3). Contudo, a construção dos respectivos controles deve ser considerada e formalizada pelo processo de gestão de riscos associado, tendo como suporte os pilares definidos pelas três dimensões básicas: tecnologia, processos e pessoas. Com isso, será possível manter a disponibilidade, a confidencialidade e a integridade das informações que serão tratadas por esses controles (Nakamura, 2007).

A análise realizada nesta seção permitiu verificar que de fato, os aspectos sobre backup e recuperação de dados relacionados à dimensão "tecnologia" estão cobertos pelos manuais dos sistemas SCADA. Contudo, há de se ressaltar que a implementação de um processo de backup e recuperação de dados que utilize e valide essas funcionalidades depende do planejamento e operação de cada organização. Isso inclui garantir que as pessoas

consigam executar o processo de acordo com o que foi definido e que estejam preparadas em operar as funcionalidades de restauração de dados em caso de materialização de algum risco.

5. Conclusões

Esse trabalho teve como objetivo avaliar a abrangência dos procedimentos de backup e recuperação de dados disponíveis no sistema SCADA, verificando sua conformidade com os controles do grupo 11 do *framework* CIS CSC, que versam sobre backup e recuperação de dados. O trabalho foi conduzido analisando o manual de referência do Sistema SCADA da Siemens WinCC V7.5 SP2, sistema muito utilizado no ambiente do setor elétrico brasileiro.

Por meio de técnicas de análise de conteúdo foi possível verificar que, apesar de o sistema possuir as funcionalidades necessárias para a realização dos procedimentos, não é possível garantir que eles são devidamente executados pelas empresas de geração, transmissão e distribuição de energia elétrica já que é necessário que as funcionalidades existentes nesses manuais sejam suportadas por processos de backup e recuperação de dados, e por sua execução e/ou monitoração efetiva de pessoas capacitadas.

Das 14 categorias iniciais identificadas, pôde-se perceber que 11 delas estavam associadas ao processo de geração de backup (externo ou interno) e as outras 03 associadas à recuperação de dados. Isso mostra que o sistema SCADA tem as funcionalidades necessárias para se garantir o processo de recuperação de dados definido no Macrocontrole 11 do CIS CSC, no entanto os instrumentos para a realização da gestão dessas funcionalidades não se apresenta de forma prática por meio de controles específicos.

Isto posto, a ausência de controles de backup e recuperação de dados no ARCiber sugere uma lacuna que precisa ser enfrentada pelas empresas Geradoras, Transmissoras e Distribuidoras de Energia Elétrica, sob supervisão e auditoria do ONS. Espera-se que uma próxima versão do ARCiber normatize esse ponto.

A perda definitiva das informações de usuários e de processsos do Sistema SCADA, em tempo real, podem provocar interrupções no fornecimento de energia elétrica e um tempo de recomposição demasiadamente grande, causando grandes prejuízos aos consumidores e às empresas concessionárias.

A relevância desse trabalho está em suscitar, portanto, o debate sobre a necessidade de revisão da RO-CB.BR.01, uma vez que a ausência de controles de Recuperação de Dados no ambiente regulado ARCiber, apesar do sistema SCADA possuir capacidade de atender aos subsídios definidos pelos Subcontroles do Macrocontrole Nº. 11 do Framework CIS CSC, eles não são evidenciados, levando a uma grande fragilidade ao processo de gestão de riscos cibernéticos do sistema elétrico de potência.

Por fim, esse trabalho oferece uma contribuição ao processo de avaliação dos riscos cibernéticos a que está submetida a infraestrutura operacional do Sistema Elétrico Brasileiro - SEB, diante das recentes ações do ONS.

Uma evolução do presente estudo pode ser sugerida como trabalho futuro, no sentido de se avaliar outros Macrocontroles do Framework CIS CSC, para os quais o ARCiber do ONS também não tenha previsto controles em seu processo de gestão de riscos cibernéticos, proposto por meio da Rotina Operacional RO-CB.BR.01 Revisão 00.

Agradecimentos

O autor Eduardo de Oliveira Lima agradece o suporte da Universidade de Brasília, por meio do DPG, Edital 01/2022; da ENBPar – Empresa Brasileira de Participações em Energia Nuclear e Binacional S/A. O autor Rafael Rabelo Nunes agradece o suporte do Centro Universitário Atenas; da Universidade de Brasília, por meio do Edital DPI/DPG 02/2022. Os autores Fernando Rocha Moreira e Rafael Rabelo Nunes agradecem o suporte do Ministério da Justiça e Segurança Pública representado pela Diretoria de Tecnologia da Informação e Comunicação (TED DTIC/SE/MJSP 01/2019). O autor Fernando Rocha Moreira agradece o suporte da FAP/DF, por meio do Edital 07/2022.

Referências

Accenture Security, (2019). The Cost of Cybercrime, Traverse City, Michigan: Ponemon Institute, from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Alcaraz, C; & Zeadally, S., (2015). “Critical infrastructure protection: Requirements and challenges for the 21st century”. International Journal of Critical Infrastructure Protection, Vol. 8, Pages 53-66. DOI: 10.1016/j.ijcip.2014.12.002

Bardin, L., (2011). Análise de Conteúdo. São Paulo: Edições 70.

CIS CSC - Center for Internet Security, (2021). “Simplified & Prioritized Cyber Defense Guidance”, CIS CSC Critical Security Controls Version 8.

Cooper, D. R.; Schindler, P. S. (2016). “Métodos de Pesquisa em Administração”, 12ª Edição. [S.l.]: McGraw Hill Brasil.

Countwordsfree, (2022). “Text Processing Tools”, from https://countwordsfree.com/

DHS CSSP - Common Cybersecurity Vulnerabilities in Industrial Control Systems, Department of Homeland Security, 92011). “Control Systems Security Program”.

Daneels, A., Salter. W., (1999). “What is Scada?”, International Conference on Accelerator and Large Experimental Physics Control Systems, Trieste, Italy.

Fossà, M. I. T., (2003). “Proposição de um constructo para análise da cultura de devoção nas empresas familiares e visionárias”. Tese (Doutorado em Administração). Universidade Federal do Rio Grande do Sul, Porto Alegre.

Ibrahim, A. I. G., (2021). "Cybersecurity: Panorama and Implementation in 2021", Safety and Security Engineering IX, WIT Transaction on the Built Envinonment, Vol. 206, WIT Press. DOI: 10.2495/SAFE210041

Plèta, T., Tvaronavičienė, M., Casa, S., Agafonov, K., (2021). "Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases". HAL Open Science. HAL: hal-03271856

Laprie, J. C., Kanoun, K., Kaanishe, M. (2007). "Modelling interdependencies between the electricity and information infrastructures", in Computer Safety, Reliability, and Security, ed: Springer, pp. 54-67, DOI:10.1007/978-3-540-75101-4_5.

Marconi, M. L.; Cientifica, E. F. da M. , (2003). 5ª edição, editora atas sa. São Paulo.

Mozzato, A. R; & Grzyboviski, D., (2011). "Análise de Conteúdo como Técnica de Análise de Dados Qualitativos no Campo da Administração: Potencial e Desafios". Revista de Administração Contemporânea, Curitiba, v. 15, n. 4.

Muncaster, P., (2014). "Microsoft Zero Day Traced to Russian 'Sandworm' Hackers," Infosecurity Magazine.

Nakamura, E.; de Geus, P. L. (2007). "Segurança de Redes em Ambientes Cooperativos". São Paulo: Novatec.

NIST, (2018). "Framework for Improving Critical Infrastructure Cybersecurity", from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Operador Nacional do Sistema Elétrico – ONS, (2021). "Manual de Procedimentos da Operação Módulo 5 - Submódulo 5.13, Número RO-CB.BR.01, Rev. 00, Item 4.1.11".

Prodanov, C. C.; Freitas, E. C. D. (2013). "Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico", 2ª Edição. [S.l.]: Editora Feevale

Scada System Siemens WinCC V7.5 SP2, (2020). SCADA WinCC: Working with WinCC, ASE50503017-AA.

Souza, J. R., Santos, S. C. M., (2020). "Análise de conteúdo em pesquisa qualitativa: modo de pensar e de fazer", Pesquisa e Debate em Educação, Juiz de Fora: U FJF, v. 10, n. 2.

Sridhar, S., Hahn, A., Govindarasu, M., (2012). "Cyber–physical system security for the electric power grid", Proceedings of the IEEE, vol. 100, pp. 210-224. DOI: 10.1109/JPROC.2011.2165269

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A., (2015). "Guide to industrial control systems (ICS) security", NIST Special Publication, vol. 800-82. DOI: 10.6028/NIST.SP.800-82r2

USCERT - United States Computer Emergency Readiness Team, (2018). Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, from https://www.us-cert.gov/ncas/alerts/TA18-074A

Vergara, S. C., (2006). "Projetos e relatórios de pesquisa". São Paulo: Atlas