# UMA RETROSPECTIVA SOBRE OS ATAQUES CIBERNÉTICOS AO SETOR ELÉTRICO EM UM CENÁRIO GLOBAL E NACIONAL

**Emanuela Paranhos Lima**
Universidade Federal da Bahia (UFBA)

**Vitaly Félix Rodríguez Esquerre**
Universidade Federal da Bahia (UFBA)

**RESUMO:** Com o avanço da automação do setor elétrico, as concessionárias estão sendo alvos de ataques cibernéticos ao redor do mundo. Quanto maior a maturidade cibernética, menores são os prejuízos decorrentes desses tipos de incidentes. A confiabilidade da operação, seja por acesso remoto ou intrusão física, pode ter impactos significativos, incluindo perda de capacidade de geração ou distribuição de energia, danos físicos aos seus equipamentos e risco a vidas humanas. Este trabalho faz uma revisão com base de dados acadêmicos (*IEEE Xplore* e *ScienceDirect*) dos principais ataques ao setor elétrico dos últimos 25 anos no cenário internacional, destacando a importância da Rotina Operacional RO-CB. BR.01 do ONS no que tange a proporcionar mitigação de riscos, aumentar a proteção da infraestrutura crítica, salvaguardando a economia, a segurança pública e o bem-estar da sociedade brasileira.

**PALAVRAS-CHAVE:** Cibersegurança, ONS, Setor Elétrico, Redes Inteligentes, Energia.

## INTRODUÇÃO

O setor elétrico de potência engloba geração, transmissão, distribuição e comercialização de energia elétrica. Machado *et al.* (2016) afirmam que com as Redes Inteligentes ou *Smart Grids* houve modernização da infraestrutura de comunicação para possibilitar o gerenciamento do trânsito bidirecional de eletricidade de todas as fontes de geração, garantindo um fornecimento contínuo de energia elétrica. Para tal, é necessária a introdução de novos componentes de comunicação para automatizar relés e chaves seccionadoras instalados em postes das distribuidoras ou medidores de energia para microgeração de consumidores. Ainda segundo Machado *et al.* (2016), a escalada de novos dispositivos nas redes elétricas que na maioria dos casos dependem de soluções públicas e protocolos baseados na Internet, traz consigo maior incidência de ataques cibernéticos. Esses ataques podem causar danos físicos e financeiros, ocasionando a interrupção dos serviços do sistema de energia conforme abordado por Rekeraho *et al.* (2023).

A segurança cibernética para infraestruturas críticas, diferente da tradicional de TI (Tecnologia da Informação), deve priorizar a disponibilidade da operação dos sistemas da rede elétrica à confidencialidade e integridade das informações transmitidas de acordo com Machado *et al.* (2016). Reconhecendo que a segurança nacional e econômica de um país depende da funcionalidade confiável do setor elétrico, o ONS (2021) ou Operador Nacional do Sistema Elétrico publicou em 2021 a Rotina Operacional (RO) que traz controles de cibersegurança a fim de aumentar a proteção da rede dos agentes.

Dessa forma, este trabalho tem como objetivo realizar uma revisão dos principais ataques ao setor elétrico no mundo e seus impactos, estabelecendo uma análise de como os critérios impostos na Rotina Operacional do ONS poderiam ter mitigado esses incidentes.

## METODOLOGIA

A metodologia empregada neste estudo para o levantamento dos principais incidentes cibernéticos no setor elétrico foi desenvolvida com base de dados acadêmicos, como *IEEE Xplore* e *ScienceDirect*, em uma abordagem de pesquisa em livros, relatórios técnicos e artigos científicos publicados nos últimos 25 anos, abrangendo incidentes reportados globalmente. A seleção dos casos foi limitada a documentos cujas palavras-chave incluíam combinações como "*cybersecurity incidents", "cyber attacks", "smart grids",* "*renewable energy*", "*hydropower", "photovoltaic"* e *"solar wind"*. Na sequência, foi realizada a categorização por tipos de ataques. As considerações finais destacam como os controles da RO do ONS mitigariam os riscos cibernéticos, caso aplicadas corretamente.

### Revisão dos principais ataques ao setor elétrico no cenário global

Dois dias antes do Natal de 2015, uma empresa de energia localizada no oeste da Ucrânia sofreu uma queda de energia que impactou cerca de 250 de mil ucranianos por até seis horas. De acordo com Hemsley e Fisher (2018), o ataque cibernético desarmou disjuntores em 30 subestações que incluíam a capital regional de Ivano-Frankivsk. Ainda segundo Hemsley e Fisher (2018), o SCADA (*Supervisory Control and Data Acquisition* - Controle de Supervisão e Aquisição de Dados) ficou inoperante e a restauração de energia teve que ser concluída manualmente, atrasando ainda mais a restauração. Um e-mail de *Spear Phishing* foi enviado para funcionários de TI e usando o *BlackEnergy Malware* para explorar macros no Microsoft Excel, os atacantes obtiveram acesso às credenciais de acesso ao sistema desses usuários. Segundo Jewkes e Vukmanovic (2017), os invasores haviam se infiltrado cerca de seis meses antes do incidente.

Freeman *et al*. (2024) informaram que um ataque *DDoS* (*Distributed Denial of Service* - Negação Distribuída de Serviço), no final de 2015, teve como alvo um *gateway* de Internet usado para controlar uma rede elétrica do Báltico, interrompendo as operações, mas não causando apagões.

Os invasores usaram o *Malware Industroyer* para controlar dispositivos em uma subestação localizada em Kiev em dezembro de 2016. Este *Malware* permitiu interação direta com dispositivos ICS (*Industrial Control Systems*) por meio de protocolos industriais e alterou seus estados (por exemplo, disjuntores de circuito fechado foram abertos), resultando em uma queda de energia. Os invasores também lançaram um ataque de Negação de Serviço Telefônico (TDoS) contra o *call center* da concessionária para impedir que os clientes relatassem a queda, prolongando a interrupção conforme informado por Hemsley e Fisher (2018). Na maioria dos casos, a energia foi restaurada em três horas, mas em outros, foi necessário ir até as subestações para fechar manualmente os disjuntores que os atacantes tinham aberto remotamente. Este segundo ataque na Ucrânia foi muito mais sofisticado do que o primeiro ocorrido em 2015.

O maior proprietário privado de ativos solares operacionais nos EUA sofreu um ataque de negação de serviço (DoS - *Denial of Service*) em março de 2019, de acordo com Dubasi et al. (2021). Semelhante ao incidente do Báltico, não houve interrupção, mas os operadores da rede perdem a comunicação com os locais de geração solar e eólica por cerca de cinco minutos com reinicialização contínua por um período de 12 horas. Isso impactou a visibilidade da empresa em cerca de 500 MW de energia eólica e fotovoltaica. Este ataque foi conhecido como o primeiro em empresas renováveis. A *North American Electric Reliability Corporation* - NERC (2019) recomendou fortemente que as concessionárias mantivessem os *firewalls* corrigidos e atualizados porque os invasores exploraram uma vulnerabilidade conhecida em um *firewall* Cisco não corrigido.

Em novembro de 2019, surge o *Ransomware Maze* que explora vulnerabilidades RDP (*Remote Desktop Protocol*) para acessar redes remotamente através da prática de força bruta e copia dados (informações legais, registros de recursos humanos, propriedade intelectual etc.) de sistemas antes de criptografá-los, mantendo os arquivos para resgate como informam Chimmanee e Jantavongso (2014). Com o início da pandemia de COVID-19 e a necessidade do trabalho remoto, as empresas em todo o mundo liberaram o uso do protocolo RDP para fornecer acesso aos seus funcionários e com o consequência abriram portas aos invasores. Como exemplo, Chimmanee e Jantavongso (2014) reportaram o caso de uma empresa estatal tailandesa responsável por fornecer eletricidade em 74 províncias do país por meio de usinas hidrelétricas, térmicas e de energia renovável teve seus arquivos criptografados pelo *Ransomware Maze* e expostos na dark web.

Brito (2020) do portal especializado em cibersegurança *Ciso Advisor* noticiou que em 2020, seis empresas de distribuição no Brasil revelaram ataques cibernéticos por *Ransomware*. Cerca de 10 TB de dados sensíveis foram criptografados e o valor do resgate chegou a quase dez milhões de dólares, como informa outra matéria da *Ciso Advisor* (2020). O maior grupo empresarial não governamental de eletricidade que atua em 11 estados brasileiros foi atacado pela exploração de uma vulnerabilidade no *JBoss*, um servidor de código aberto baseado em Java. Após criptografar todos os servidores da empresa, os atacantes teriam pedido um resgate equivalente a R$5 milhões em Bitcoins. A empresa levou uma semana para restaurar os sistemas de TI conforme noticiado por Caram (2020).

A administração de um município dos EUA teve seus sistemas de rede elétrica desligados por um atacante, em agosto de 2020, possivelmente via um golpe de *Phishing* ou ataque de força bruta. O resgate foi pago no valor de US$45.000 após a cidade não conseguir restaurar os sistemas a partir de seus backups, de acordo com o relatório da Kaspersky (2021).

Ainda segundo o mesmo relatório da Kaspersky (2021), em setembro de 2020, uma empresa de fornecimento de eletricidade no Paquistão foi alvo de um ataque de *Ransomware Netwalker* que disponibilizou 8,5 GB de arquivos de dados financeiros e de dados sensíveis de seus 2,5 milhões de clientes. Foram solicitados quase quatro milhões de dólares como resgate desses dados. Este incidente ocasionou uma interrupção do faturamento e dos serviços online da empresa, mas o fornecimento de energia e serviços críticos ao cliente estavam totalmente funcionais.

Um ataque cibernético paralisou cerca de 6 mil turbinas eólicas em toda a Europa em fevereiro de 2022, afetando uma potência total instalada de mais de 10GW. A rede de notícias *Wind Fair* (2022) noticiou que a operadora das turbinas havia relatado que o monitoramento remoto e o controle pararam de funcionar devido a uma falha na conexão via satélite com seus sistemas. Os serviços de comunicação fornecidos via satélite caíram simultaneamente quando as tropas russas invadiram a Ucrânia. De acordo com a agência governamental americana CISA (2022), os invasores russos exploraram uma configuração incorreta de VPN (*Virtual Private Network* - Rede Privada Virtual) que permitiu movimentação lateral pela rede e possibilitou sobrescrever dados em mais de 40.000 modems de clientes.

Na madrugada do dia 12 de abril de 2022, o monitoramento remoto de turbinas de um parque eólico alemão sofreu um ataque cibernético, levando cerca de 02 dias para recuperar o sistema e as atividades operacionais conforme informativo da própria companhia Deutsche Windtechnikl (2022). Nessa mesma data, o órgão *Computer Emergency Response Team* da Ucrânia ou CERT-UA (2022) relatou que um agente malicioso da equipe russa *Sandworm* teve como alvo vários elementos críticos de infraestrutura, incluindo subestações elétricas de alta tensão, usando um *Malware* chamado *Industroyer2* (uma variante do *software* malicioso usado no ataque de 2016). O ataque foi mitigado antes de causar um apagão que poderia impactar aproximadamente dois milhões de pessoas como noticiado pela agência de notícias IronNet (2022).

O *Ransomware BlackBasta* foi utilizado para atacar uma empresa de energia italiana afetando os servidores do *software* de virtualização em 2 de fevereiro de 2023. De acordo com Hernandez (2023), o fabricante do *software* havia lançado *patches* para essa vulnerabilidade 02 anos antes. O sistema de TI da empresa caiu, mas a infraestrutura operacional não foi danificada. A exploração massiva dessa vulnerabilidade também ocorreu em corporações de outros países como França (188 instâncias), Alemanha (91 instâncias) e Estados Unidos (69 instâncias).

Freeman *et al*. (2024) informaram que 22 empresas dinamarquesas de energia foram comprometidas em maio de 2023 por vulnerabilidades não corrigidas e uma vulnerabilidade de zero-day em *firewalls* Zyxel que permite que invasores remotos obtenham controle total do sistema de segurança sem autenticação. Algumas organizações perderam visibilidade para conexões remotas. Este incidente na infraestrutura crítica da Dinamarca é considerado o maior ataque online do país, embora não tenha havido impacto material significativo nas operações de energia. Em alguns casos, as organizações afetadas foram forçadas a entrar em um modo de operação isolado.

## Cenário nacional de segurança cibernética no setor elétrico

No Brasil, por suas dimensões continentais, as usinas geradoras de energia localizadas em áreas remotas se conectam aos centros de consumo através do Sistema Interligado Nacional (SIN). De acordo com Branquinho e Leal (2022), são mais de 145 mil km de linhas de transmissão interligando os agentes de energia e a rede do ONS. Essa teia facilita a disponibilização de energia por todo o país, porém evidencia uma dependência entre o ecossistema: caso um desses agentes seja impactado, todo o SIN será afetado. Branquinho e Leal (2022) alertam sobre o risco sistêmico do SIN no que tange a segurança cibernética.

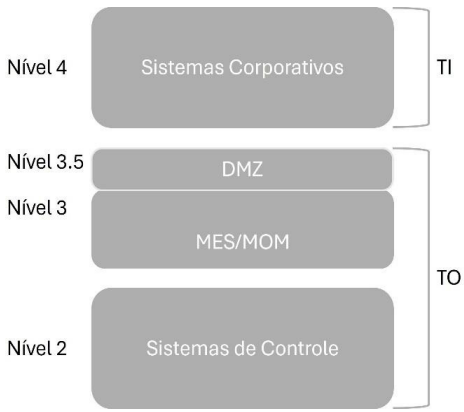


**Figura 1 –** Arquitetura definida pela Rotina Operacional do ONS com base no Modelo *Purdue* (ISA-99).

**Fonte:** Adaptado de Branquinho e Branquinho (2021, p. 43).

Dessa forma, o Operador Nacional do Sistema – ONS (2021) divulgou a Rotina Operacional RO-CB.BR.01 como um marco para a segurança cibernética do setor elétrico no Brasil em julho de 2021. O objetivo era garantir que os agentes executassem 18 controles de segurança no ambiente regulado cibernético chamado de ARCiber em duas ondas de implementação (18 e 24 meses após a entrada em vigor do documento). As seis categorias de controles são:

- Arquitetura Tecnológica para o Ambiente: redes segregadas de acordo com a *Purdue Reference Model* (Figura 1), acesso ao ARCiber a partir de redes externas somente via VPN e não deve ser acessível através da internet e implementar soluções *Antimalware* (*Application Whitelisting*);
- Governança de Segurança da Informação: definição de papéis e responsabilidades, além de um gestor e um suplente responsáveis pela segurança cibernética do ARCiber;
- Inventário de Ativos: ativos devem ser inventariados a cada 24 meses, de forma segura e padrões de configuração segura (*hardening*) devem ser criados;
- Gestão de Vulnerabilidades: gestão de pacotes de correção de segurança (*patches*) com cronograma de implementação das correções para ativos novos e em operação;
- Gestão de Acessos: política de gestão de acessos e identidades individuais e aprovadas pela alçada competente deve seguir o princípio de minimização (somente deve-se conceder o acesso mínimo necessário) e utilização de múltiplos fatores de autenticação (MFA);
- Monitoramento e Resposta a Incidentes: dispositivos de segurança como *Firewalls,* IDS (*Intrusion Detection System* - Sistema de Detecção de Intrusão), IPS (*Intrusion Prevention System* - Sistema de Prevenção de Intrusão) e *Antimalware* devem estar configurados para gerar logs de segurança e alertas, implementação de plano de resposta a incidentes com testes de ativação periódicos e notificação ao ONS em caso de incidentes cibernéticos que afetem ativos do ARCiber.

Os controles da RO passeiam pelos três pilares da segurança cibernética: pessoas, processos e tecnologia. Há um tratamento de exceção para os casos em que os requisitos não podem ser implementados. Para cada exceção gerada, uma documentação detalhada deve ser criada.

## RESULTADOS E DISCUSSÕES

Os principais ataques cibernéticos no setor de energia elétrica no período de 2015 a 2023, descritos na Seção 2.1, são mostrados de forma geográfica na Figura 2. Observa-se a concentração de ataques em países com histórico de conflitos geopolíticos, como a Ucrânia. Branquinho e Branquinho (2021, p. 55) trazem o conceito de quinta dimensão da guerra, onde a ofensiva se dá em espaço cibernético através de descoberta de vulnerabilidades e exploração de falhas de segurança. Outro recorte, conforme Figura 3, aponta o crescente quantitativo de incidentes durante o período da pandemia de COVID-19 em decorrência do teletrabalho. O relatório geral de riscos da *World Economic Forum* de 2020 trouxe os ataques cibernéticos no top 10 de acordo com Branquinho e Branquinho (2021, p. 55).


**Figura 2 –** Os principais ataques cibernéticos no setor de energia no período 2015-2023.

**Fonte:** Produzido pelo autor.

A arquitetura do ARCiber é o primeiro ponto crucial abordado na RO e refere-se a segregação de redes, além de limitar a exposição de dispositivos voltados para a Internet. Um exemplo de incidente onde esse controle não foi bem aplicado, foi o *Spear Phishing* usando o *BlackEnergy Malware* na Ucrânia em 2015, descrito na Seção 2.1, onde o ataque tem origem na rede de TI devido a maior exposição às redes externas e a um maior número de usuários e servidores. Na Figura 1, é possível ver a segmentação das zonas em Sistemas de Controle, MES (*Manufacturing Execution System* - Sistema de Execução de Manufatura), MOM (*Manufacturing Operation Management* - Sistemas de Gestão de Operações) e DMZ (*Demilitarized Zone* - Zona Desmilitarizada) na TO (Tecnologia Operacional) e Sistemas Corporativos na TI. Essa segregação quando bem implementada impede que um ataque se espalhe da rede corporativa para rede operativa do sistema elétrico. Reduzir essa superfície de ataque auxilia significativamente na resposta e recuperação de incidentes.

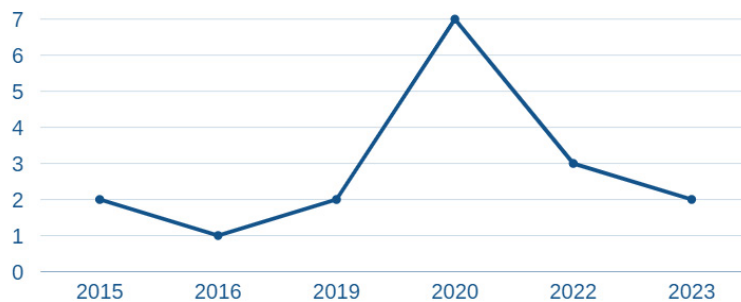


**Figura 3 –**Representação de ataques cibernéticos no setor de energia no período 2015- 2023.

**Fonte:** Produzido pelo autor.

A identificação de ativos (*hardware* e *software*) é um componente chave no gerenciamento de risco de segurança cibernética. Os principais ataques cibernéticos exploram vulnerabilidades previamente divulgadas, o que torna essencial a existência de estratégias de gestão de *patches* como descrito na RO. A política de segurança da organização para todas as tecnologias conectadas ao ARCiber deve incluir pelo menos o mapeamento de ativos inventariados para os lançamentos de *patches* do fornecedor e um cronograma para implementar as correções. Exemplos de eventos onde esse controle não foi robusto o suficiente ou inexistente são os incidentes ocorridos com a empresa de energia italiana com a vulnerabilidade conhecida no *software* de virtualização e com as empresas de energia dinamarquesas e americana com vulnerabilidades em *firewalls,* como descrito na Seção 2.1.

De acordo com informações publicadas por Branquinho e Branquinho (2021, p. 319), em 2015, os cibercriminosos obtiveram acesso às credenciais do sistema da empresa de energia ucraniana. Se todos os controles exigidos na RO fossem implementados naquela organização, esse ataque não teria êxito, porque seria necessário que o invasor também possuísse o token MFA além da credencial. O mesmo se aplica aos casos de *Ransomware* das corporações da Tailândia, Paquistão e Brasil. Autenticação multifator é uma tecnologia de segurança que utiliza múltiplos métodos de autenticação para verificar a identidade do usuário conforme explicam Branquinho e Branquinho (2021, p. 265) no usando as seguintes premissas:

- Algo que você sabe: credencial ou PIN;
- Algo que você tem: token, smartphone ou uma chave USB segura;
- Algo que você é: impressão digital, escaneamentos de retina ou reconhecimento de voz / facial.

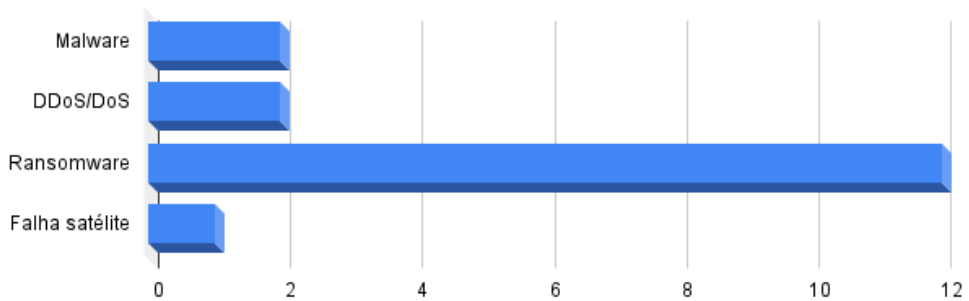


**Figura 4 –** Representação dos tipos de ataques cibernéticos no setor de energia no período de 2015 a 2023.

**Fonte:** Produzido pelo autor.

Para cumprir todos os controles da RO, Branquinho e Leal (2022) advertem que as empresas precisam investir em sua infraestrutura, políticas de segurança e conscientização dos funcionários. No entanto, a legislação atual não prevê a remuneração para as concessionárias na tarifa de energia para os investimentos realizados na RO. A falta de orçamento das empresas de energia em projetos de segurança se torna um grande desafio para a implementação dos controles. A situação é ainda pior quando se discute sobre empresas públicas.

Outro ponto de crítica a RO, é a ausência de controles referentes a gestão de acesso físico. Por se tratar de um setor ao qual as subestações são automatizadas e por consequência não há operadores locais, infraestruturas com baixa ou nenhuma segurança física facilitam que invasores tenham acesso aos sistema de controle e possam lograr um ataque cibernético. Controles como bloqueio de portas USB, utilização de *racks* com portas e chaves armazenadas em um claviculário com responsabilidade da alçada competente e bloqueio de portas *Ethernet* não utilizadas de elementos de rede (switches, roteadores e *firewalls*) são fundamentais para a robustez da gestão de acesso físico.

Alguns controles possuem pouco aprofundamento técnico ou ausência de detalhamento de como devem ser realizados. Um exemplo é o item de Monitoramento e Resposta a Incidentes que não inclui diretamente a realização de *backup*. Como abordam Branquinho e Branquinho (2021, p. 265), a realização da cópia de segurança deve ser realizada de forma periódica utilizando ferramenta automática ou de forma manual e deve ser estabelecido um cronograma de restauração para garantir a integridades da informação copiada. Outra recomendação de Branquinho e Branquinho (2021, p. 265) é o armazenamento dos *backups* em ambiente fora da unidade para casos de recuperação de desastres ou DRP (*Disaster Recovery Plan*).

## CONCLUSÕES E/OU CONSIDERAÇÕES FINAIS

Os resultados evidenciaram que os ataques cibernéticos contra empresas de energia e seus *stakeholders* cresceram substancialmente com impactos significativos na operação, segurança e confiabilidade do sistema elétrico impulsionado pela crescente digitalização do setor. No período da pandemia de COVID-19, devido a necessidade de distanciamento social, muitas companhias liberaram acesso remoto sem estar completamente estruturada e acabaram abrindo portas de entrada para invasores mal-intencionados.

Como consequência, as empresas buscaram elevar o seu nível de maturidade se apoiando em *Frameworks* de segurança cibernética, além do uso de recursos tecnológicos para proteger seus ativos de ataques. Em alguns países, há regulamentações para o setor elétrico que impulsionam esse crescimento na conscientização e investimento em proteção cibernética, como exemplo dos EUA com NERC-CIP e da Europa com NIS2 (voltado para toda infraestrutura crítica, não apenas o setor elétrico).

Para o Brasil, a partir de 2021, os agentes do setor elétrico precisaram se ajustar à Rotina Operacional do ONS, que foi construída à luz dos principais *Frameworks* de segurança. Esse marco regulatório brasileiro gerou uma grande disrupção para aquelas empresas que não tinham a área de segurança cibernética de OT estruturada (pessoas, processos e tecnologias).

A análise dos casos estudados revelou que os incidentes poderiam ter sido mitigados ou evitados com o cumprimento dos critérios de segurança cibernética da RO do ONS, comprovando a efetividade desse marco regulatório brasileiro. No entanto, constatou-se que o grande desafio é a ausência de investimentos adequados em infraestrutura, políticas de segurança e conscientização dos funcionários.

## REFERÊNCIAS


BRANQUINHO, T.; BRANQUINHO, M. **Segurança Cibernética Industrial: as infraestruturas críticas mundiais correm perigo. Aprenda a proteger redes e sistemas de controle com uma metodologia comprovada na prática**. Alta Books, Rio de Janeiro, 2021. p. 43-53.

BRANQUINHO, T.; BRANQUINHO, M. **Segurança Cibernética Industrial: as infraestruturas críticas mundiais correm perigo. Aprenda a proteger redes e sistemas de controle com uma metodologia comprovada na prática**. Alta Books, Rio de Janeiro, 2021. p. 55-69.

BRANQUINHO, T.; BRANQUINHO, M. **Segurança Cibernética Industrial: as infraestruturas críticas mundiais correm perigo. Aprenda a proteger redes e sistemas de controle com uma metodologia comprovada na prática**. Alta Books, Rio de Janeiro, 2021. p. 265-283.

BRANQUINHO, T.; BRANQUINHO, M. **Segurança Cibernética Industrial: as infraestruturas críticas mundiais correm perigo. Aprenda a proteger redes e sistemas de controle com uma metodologia comprovada na prática**. Alta Books, Rio de Janeiro, 2021. p. 319-327.

BRANQUINHO, M; LEAL, R. **Capítulo VII - Ambiente regulatório de segurança cibernética para empresas de energia no Brasil**. *O Setor Elétrico*. Fascículo Segurança cibernética, v. 190, p. 30–32, 2022. Disponível em: https://www.osetoreletrico.com.br/capitulo-vii-ambiente-regulatorio-de-seguranca-cibernetica-para-empresas-de-energia-no-brasil/ Acesso em: 10 jun. 2024.

BRITO, P. **Ransomware Maze anuncia invasão nas redes da CPFL e da LG**. *Ciso Advisor*, 2020. Disponível em: https://www.cisoadvisor.com.br/Ransomware-maze-anuncia-invasao-nas-redes-da-cpfl-e-da-lg-electronics/. Acesso em: 10 jun. 2024

CARAM, L. **Grupo Energisa, que fornece energia a 18 estados do Brasil, sofre ataque hacker pedindo R$ 5 milhões em BTC**. *Cointelegraph*, 2020. Disponível em: https://br.cointelegraph.com/news/energy-company-energisa-suffers-hacker-attack-asking-for-r-5-million-in-bitcoin. Acesso em: 10 jun. 2024.

CERT-UA. **Cyber attack of the Sandworm group (UAC-0082) on energy facilities of Ukraine using malware INDUSTROYER2 and CADDYWIPER (CERT-UA#4435).** *CERT-UA*, 2022. Disponível em: https://cert.gov.ua/article/39518. Acesso em: 10 jun. 2024.

CHIMMANEE, K.; JANTAVONGSO, S. **Digital forensic of Maze Ransomware: A case of electricity distributor enterprise in ASEAN**. *Expert Systems With Applications*, v. 249, Part B, 2024. doi. org/10.1016/j.eswa.2024.123652

CISA. U.S. **Government Attributes Cyberattacks on SATCOM Networks to Russian State-Sponsored Malicious Cyber Actors**. *CISA*, 2022. Disponível em: https://www.cisa.gov/news-events/alerts/2022/05/10/us-government-attributes-cyberattacks-satcom-networks-russian-state. Acesso em: 10 jun. 2024.

CISO ADVISOR. **EDP comunica oficialmente invasão e vazamento de dados de sua rede.** *Ciso Advisor*, 2020. Disponível em: https://www.cisoadvisor.com.br/edp-comunica-oficialmente-invasao-e-vazamento-de-dados-de-sua-rede/. Acesso em: 10 jun. 2024.

DEUTSCHE WINDTECHNIKL. **Cyber attack on Deutsche Windtechnik.** *Deutsche Windtechnikl*, 2022. Disponível em: https://www.deutsche-windtechnik.com/nl/news/press-releases/detail/cyber-attack-on-deutsche-windtechnik/. Acesso em: 10 jun. 2024.

DUBASI, Y.; KHAN, A.; LI, Q.; MANTOOTH, A. **Security Vulnerability and Mitigation in Photovoltaic Systems.** *IEEE 12th international Symposium on Power Electronics for Distributed Generation Systems (PEDG)*. Chicago, p. 1-7, Jun. 2021. doi: 10.1109/PEDG51384.2021.9494252

FREEMAN, S. G.; KRESS-WEITENHAGEN, M. A.; GENTLE, J. P.; CULLER, M. J.; EGAN, M. M.; STOLWORTHY, R. V. **Attack Surface of Wind Energy Technologies in the United States**; Idaho National Laboratory, Jan. 2024. https://doi.org/10.2172/2297403.

HEMSLEY, K. E.; FISHER, R. E**. History of Industrial Control System Cyber Incidents**. Idaho National Laboratory, Dez. 2018. https://doi.org/10.2172/1505628

HERNANDEZ, J. A. G.; TEODORO, P. G.; CARRION, R. M.; GOMEZ, R. R. **Crypto-Ransomware: A revision of the state of the art, advances and challenges.** *Electronics*, v. 12, n. 21, p. 1–39, 2023. doi. org/10.3390/electronics1221449.

IRONNET**. Industroyer2 malware targeting Ukrainian energy company**. *IronNet*, 2022. Disponível em: https://www.ironnet.com/blog/industroyer2-malware-targeting-ukrainian-energy-company. Acesso em: 10 jun. 2024.

JEWKES, S.; VUKMANOVIC, O. **Suspected Russia-backed hackers target Baltic energy networks.** *Reuters*, 2017. Available: https://www.reuters.com/article/us-baltics-cyber-insight/suspected-russia-backed-hackers-target-baltic-energy-networks-idUSKBN1871W5/. Acessado 10 jun. 2024.

KASPERSKY. **Principais ataques de Ransomware**. *Kaspersky*, 2021. Disponível em: https://www.kaspersky.com.br/resource-center/threats/top-ransomware-2020. Acesso em: 10 jun. 2024.

MACHADO, T. G.; MOTA, A. A.; MOTA L.T. M.; CARVALHO M. F. H.; PEZZUTO, C. C. **Methodology for the Cybersecurity Maturity Level Identification in Smart Grids**. *IEEE Latin America Transaction*, v.14, n. 11, p. 4512–4519, Nov. 2016.

NERC. **Lesson Learned: Risks posed by firewall firmware vulnerabilities.** *NERC*, Set. 2019. Disponível em: https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf. Acessado em 10 jun. 2024.

ONS. **ONS Divulga Rotina Operacional Sobre Segurança Cibernética.** *ONS*. 2021. Disponível: https://www.ons.org.br/Paginas/Noticias/20210702-rotina-operacional-seguranca-cibernetica.aspx. Acesso em: 10 jun. 2024.

REKERAHO, A.; COTFAS, D. T.; COTFAS, P. A.; BALAN, T. C.; TUYISHIME, E.; ACHEAMPONG, R. **Cybersecurity challenges in IoT-based smart renewable energy.** *International Journal of Information Security*, v. 23, p. 101-117, Ago. 2023. doi.org/10.1007/s10207-023-00732-9

WIND FAIR. **Over 95 per cent of WECs back online following disruption to satellite communication**. *Wind Fair*, 2022. Disponível em: https://w3.windfair.net/wind-energy/pr/40316-enercon-wind-turbine-wind-farm-satellite-communication-converter-disruption-remote-monitoring-scada-ka-sat-russia-ukraine-europe-access. Acesso em: 10 jun. 2024.