ESCOLA SUPERIOR DE GUERRA

RICARDO FÉRRE LACERDA FERREIRA

UTILIZAÇÃO DA ARQUITETURA *ZERO TRUST* PARA DEFESA CIBERNÉTICA DAS INFRAESTRUTURAS CRÍTICAS DO SETOR ELÉTRICO NACIONAL

Trabalho Acadêmico – Ensaio Acadêmico apresentado ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do certificado do Curso Superior de Segurança e Defesa Cibernética.

Orientador: Prof Cel R/1 João de Azevedo

Rio de Janeiro

2024

Documento assinado digitalmente
gov.br
RICARDO FERRE LACERDA FERREIRA
Data: 23/10/2024 10:38:12-0300
Verifique em https://validar.iti.gov.br

RICARDO FÉRRE LACERDA FERREIRA

RESUMO

A implementação da arquitetura de rede *Zero Trust* tem sido utilizada no sector dos Sistemas de Controle Industrial (SCI) para defender e impedir as ciberameaças ou o cibercrime. Tendo em conta a capacidade da arquitetura, é pouco provável que um único ponto de extremidade comprometido nas redes de confiança zero possa propagar-se lateralmente, infectando toda a rede, o que nos permite adotar a arquitetura no sector da energia elétrica. No Brasil não existe uma determinação do Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC) que determine a utilização desta arquitetura de micro segmentação das redes como solução necessária para realizar a defesa cibernética destas infraestruturas. A falta desta disposição, coloca a sua rede exposta a possíveis ataques cibernéticos e de seus desafios de segurança. A proteção destes sistemas físicos tem sido discutida devido o setor de energia elétrico ser alvo de ataques cibernéticos nos conflitos contemporâneos. Motivado por esta convergência, este documento tem como objetivo apresentar uma proposta de mudança na PLANSIC para adoção desta arquitetura de segurança abrangente de confiança zero para ajudar a reduzir os riscos e ajudar a proteger os sistemas físicos elétricos do Brasil e garantir a continuidade deste serviço para toda a população.

Palavras-chave: infraestrutura crítica nacional; Arquitetura de Confiança Zero (*Zero Trust)*, defesa cibernética.

ABSTRACT

The implementation of Zero Trust network architecture has been used in the Industrial Control Systems (ICT) sector to defend against and prevent cyber threats or cybercrime. Given the architecture's capabilities, it is unlikely that a single compromised endpoint in zero trust networks could spread laterally, infecting the entire network, which allows us to adopt the architecture in the electricity sector. In Brazil, there is no provision in the National Critical Infrastructure Security Plan (PLANSIC) for the use of this micro-segmentation network architecture as a necessary solution for cyber defense of these infrastructures. The lack of this provision exposes your network to possible cyber-attacks and security challenges. The protection of these physical systems has been discussed due to the electricity sector being the target of cyber-attacks in contemporary conflicts. Motivated by this convergence, this document aims to present a proposal to change PLANSIC to adopt this comprehensive zero-trust security architecture to help reduce risks and help protect Brazil's physical electrical systems and ensure the continuity of this service for the entire population.
Keywords*: national critical infrastructure; zero trust; cyber defense.*

1 INTRODUÇÃO

A segurança das Infraestruturas Críticas (IEC) passou a ser evidenciadas como uma tendência no mundo com o advento dos atentados terroristas ocorridos nos Estados Unidos da América, em 11 de setembro de 2011, conforme Decreto n° 10.569, de 9 de dezembro de 2020, que aprovou a Estratégia Nacional de Segurança das IEC (ENSIC, 2020). A partir disso, houve uma escalada mundial de ataques cibernéticos a estas IEC com o Setor energético como principal alvo. Esta afirmação pode ser consolidada observando-se os últimos acontecimentos mundiais.

Em 2015, dezenas de subestações do oeste da Ucrânia sofreram ciberataques que interrompeu o fornecimento de energia de 220.000 (vinte e dois mil) consumidores, conforme (CISA, 2016). Em 2021, a *Delta-Montrose Eletric Association* (DMEA), uma cooperativa distribuidora de energia elétrico do norte do Colorado, EUA, foi vítima de um ataque de ransomware, conforme (CCSC, 2016), que destruiu 20 a 25 anos de dados armazenados, afetou a plataforma de faturamento e obrigou o desligamento de 90% de sua rede interna de computadores, conforme (CISO, 2021).

Em 2022, outro ataque foi direcionado ao sistema elétrico ucraniano com o advento do conflito Rússia e Ucrânia, contudo, devido aos ensinamentos do ataque anterior, foi rechaçado a tempo, mas teria o potencial de atingir mais de 2 milhões de consumidores se obtivesse êxito, conforme (Ironnet Threat Research Team, 2022).

1.1 Motivação

As IEC de um País desempenham um papel fundamental tanto para o desenvolvimento econômico sustentável e integração, como para a segurança e soberania nacional. Logo, uma possível interrupção aos serviços de comunicações, de energia, de transporte, de águas, de finanças e de Defesa são fatores que podem prejudicar o adequado fornecimento de serviços essenciais e acarretar transtornos e prejuízos ao Estado, à sociedade e ao meio ambiente.

Por oportuno, conforme (Sandoval, 2023), para o Brasil deixar sua posição periférica nas cadeias globais de produto de alto valor agregado e de alta tecnologia, é necessário priorizar quatro grandes arquétipos geopolíticos, conforme figura 1.

Portanto, conforme a figura 1, o Brasil é uma superpotência energética. A principal matriz energética do Brasil está calcada nas suas usinas hidrelétricas. O que justifica uma maior atenção quanto a segurança cibernética das nossas IC responsáveis pelo setor elétrico.

Figura 1: Prioridade da estratégia nacional.

Fonte: Sandoval, (2023).

As IEC utilizam sistemas de Tecnologia Operacional (TO) e Sistemas de Controle Industrial (*Industrial Control System* - ICS), que são usados para monitorar e gerenciar dispositivos, processos e infraestruturas, e que extremamente vulneráveis à ataques cibernéticos devido às suas características de alta disponibilidade, poucas janelas de manutenção e nenhuma atualização de *firmware,* conforme (Shakarian, 2013).

Por conseguinte, a natureza dos ambientes de TO dentro das IEC torna-os particularmente vulneráveis a ameaças cibernéticas pois estes ICS são sistemas tem maior probabilidade de apresentar vulnerabilidades que podem ser exploradas por um invasor devido a serem sistemas de longa duração, não conseguirem parar para realizar a sua manutenção e atualizados com pouca frequência.

1.2 Problema de pesquisa

Dessa forma, o problema de pesquisa deste trabalho é elencar: como mitigar os ataques cibernéticos à IEC de energia elétrica do Brasil e propor uma arquitetura micro segmentada, arquitetura de Confiança Zero (*Zero Trust* - ZT), como solução?

1.3 Objetivo Geral

O objetivo final deste trabalho é entender o papel do Gabinete de Segurança Institucional (GSI) relacionando-o com as IEC, como as Forças Armadas podem apoiar o GSI na implementação de uma arquitetura de micro segmentação, implementando a ZT, nas redes de IEC e propor a adoção desta arquitetura como solução para mitigar ataques cibernéticos as IEC do sistema energético brasileiro.

Este estudo não tem o objetivo de apresentar propostas de técnicas aprofundadas para mitigar os problemas inerentes à adoção de micro segmentação entre TI e TO e nem como solucioná-los.

1.4 Objetivo Específicos

Neste cenário, este trabalho tem como objetivos específicos identificar os principais problemas na proteção cibernética a ser utilizada pelo Operador Nacional do Sistema Elétrico (ONS), entender como a Política Nacional de Segurança da IEC (PNSIC), a Estratégia Nacional de Segurança da IEC (ENSIC) e o Plano Nacional de Segurança da IEC (PlanSIC) estão desenvolvendo ações para mitigar as ameaças cibernéticas e, por fim, propor a ZT como estratégia a ser desenvolvida pelo Estado para realizar a segurança cibernética destas IEC.

1.5 Relevância do trabalho

A relevância deste estudo reside no fato de as Forças Armadas Brasileiras, em particular o Exército Brasileiro, através do Sistema Militar de Defesa Cibernética (SMDC), ter como objetivo contribuir para a proteção de infraestruturas críticas e recursos-chaves nacionais (Brasil, 2023). Neste contexto, a intenção deste trabalho é colocar uma luz sobre o tema, de forma que este assunto possa começar a ser debatido com mais propriedade e assertividade dentro do GSI/PR a fim de subsidiar futuras decisões sobre a adoção ou não da ZT para as IEC do setor energético do Brasil.

2 DESENVOLVIMENTO

Em 1990 houve uma reforma do setor elétrico no Brasil. Esta reforma permitia ações imediatas como desburocratização e modernização, prevendo a entrada de agentes privados no setor. Este movimento sistematizou leilões de energia com intuito de dar sustentabilidade nos sistemas de distribuição e transmissão do setor.

Houve, ainda, uma corrida tecnológica visando o melhor gerenciamento da rede elétrica com a mudança de dispositivos analógicos para digitais. Colocando, assim, o setor elétrico conectado às redes de telecomunicações. Com isso, não demorou muito para que o sistema elétrico fosse alvo de ataques cibernéticos.

Segundo a ENSIC, as infraestruturas de energia possuem dimensão estratégica**,** uma vez que desempenham um papel essencial tanto para segurança e soberania nacionais, como para a integração e desenvolvimento econômico sustentável do País.

Em 2021, ataques cibernéticos às empresas de elétricas como: EDP, Copel, Energisa e até mesmo a Empresa de Pesquisa Energética (EPE) chegam a interromper algumas operações devido à ataques cibernéticos no seu parque tecnológico (Ataques, 2021).

2.1 As infraestruturas Críticas Nacionais

De acordo com Decreto n° 9.573, de 22 de novembro de 2018 que aprovou a Política Nacional de Segurança das IEC (PNSIC), a definição de Infraestrutura Crítica (IEC) são instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade.

Por conseguinte, o mesmo Decreto define o conceito de interdependência de IEC como a relação de dependência ou interferência de uma infraestrutura crítica em outra ou de uma área prioritária de infraestruturas críticas em outra.

Desta forma, podemos inferir que o setor elétrico possui está interdependência entre as demais IEC previstas na ENSIC a saber: transporte, finanças e águas pois todas necessitam de energia elétrica para desempenhar suas funções.

Ademais, as IEC no Brasil foram classificadas através dos seguintes setores: comunicações, finanças, energia, transporte e águas. A responsabilidade de identificar, acompanhar e analisar o risco para garantir sua integridade e funcionamento foi passada para o Gabinete de Segurança Institucional do Presidente da República (GSI/PR).

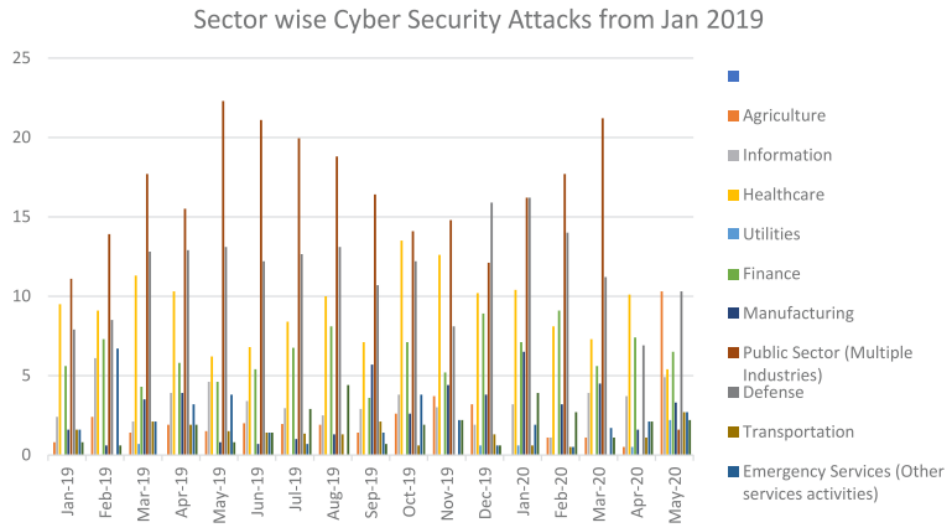
Por oportuno, as IEC de energia elétrica devem ser mantidas em funcionamento a qualquer custo para o bem da sociedade. Desta forma, uma interrupção no fornecimento de energia por violações de segurança se traduz em perdas significativas como o encerramento da produção industrial, a paralização do sistema bancário provocando perdas financeiras e até mesmo o risco de vida para os setores da saúde.

Estas violações de segurança têm sido provenientes de ciberataques. De acordo com Alagappan, Venkatachary e Andrews, (2022), 16% dos ataques a IEC foram direcionados ao setor de energia elétrica, conforme figura 2. Isto ocorre devido a digitalização das redes elétricas, mudando a dinâmica do da produção, transmissão e distribuição da energia elétrica.

Soma-se a isso, a automação dos dispositivos elétricos representa outra grande vulnerabilidade, pois os dispositivos precisam de conectividade com a Internet. Aumentando, assim, a superfície de ataque dos cibercriminosos.

Os ataques cibernéticos perpetrados aos sistemas elétricos são baseados em ataques de indivíduos *insider* ou criminosos cibernéticos. Os Insider são indivíduos de dentro da organização interessados em explorar seus privilégios específicos para prejudicar ou vazar dados confidenciais com interesses de espionagem industrial ou extorsão (Federici; Martintoni; Senni, 2023).

Figura 2: Setores que sofreram ciberataques desde Jan 2019.



Fonte: Alagappan, Venkatachary e Andrews (2022).

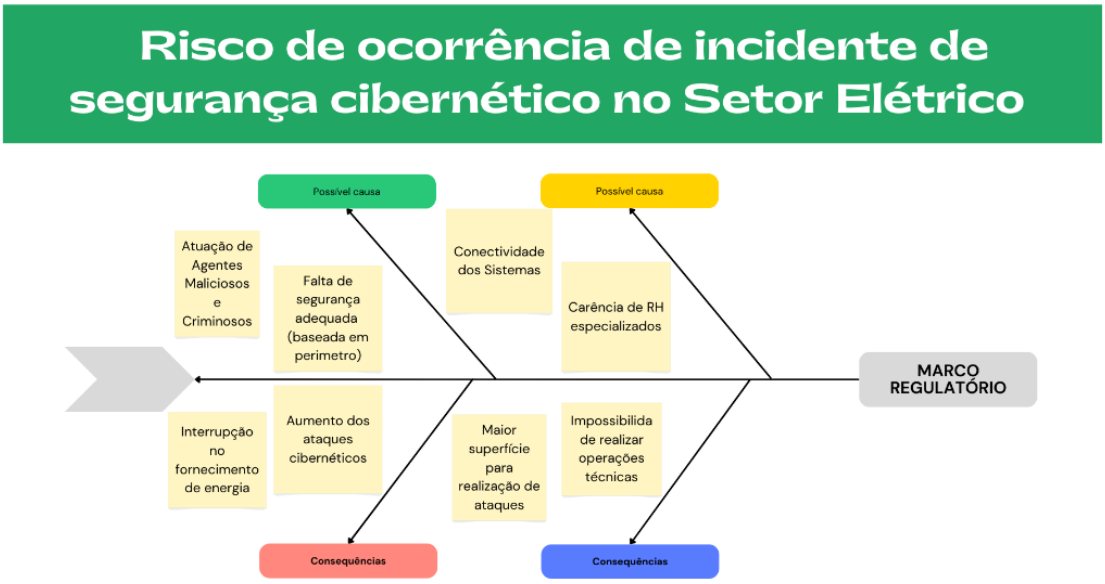
Desta forma, a estratégia de defesa cibernética baseada em perímetros de segurança não garante mais a inviolabilidade do sistema. Este modelo tradicional de segurança em camadas pressupõem um perímetro de rede com uma zona de confiança, “estratégia do castelo”, que é protegida contra acessos não autorizados. Neste modelo, qualquer indivíduo que tenha ultrapassado as “muralhas” do castelo e opere na zona de confiança é considerado confiável (Ramezanpour; Jagannath, 2022).

No entanto, devido a digitalização e automação das redes elétricas, com suas características heterogênea e dinâmica, tornam os modelos tradicionais vulneráveis a interrupção do serviço através de movimentos laterais ou engenharia social de *Insider* nas zonas de confiança após ou antes da autenticação, conforme figura 3.

Desta forma, para evitar um colapso em diversos outras IC que dependem do sistema elétrico, é necessário adotar uma arquitetura de rede onde a “confiança” não seja uma vulnerabilidade. Ou seja, é necessário implementar uma solução plausível para remover a vulnerabilidade que afeta tecnologias e pessoas, para isso propomos uma solução de arquitetura de microssegmentação de redes sem qualquer pressuposto de

confiança aos sistemas e redes adjacentes, a arquitetura *ZeroTrust* (ZT) (Je; Jung; Choi, 2021).

Figura 3: Risco de ocorrência de incidente de segurança cibernético no setor elétrico.



Fonte: O autor, 2024.

2.2 A arquitetura Zero Trust (ZT) - Confiança Zero.

A arquitetura Zero Trust (ZT) é o termo para um conjunto em evolução de paradigmas de cibersegurança que deslocam as defesas de perímetros estáticos baseados em rede para se concentrarem nos utilizadores, bens e recursos conforme a NIST (800-207) (Rose, *et.al*, 2020).

No seu cerne, a ZT assume que não é concedida nenhuma confiança implícita a bens ou utilizadores com base apenas na sua localização física ou de rede (ou seja, redes locais versus a Internet) ou propriedade de bens (empresariais ou pessoais).

A ZT utiliza autenticação multifator contínua, microssegmentação, encriptação avançada, segurança de *endpoint*, análise e auditoria robusta, entre outras capacidades, para fortalecer os dados, aplicações, ativos e serviços para garantir a resiliência cibernética.

Desta forma, a execução da ZT fornece aos destinatários dados de confiança, etiquetados e rotulados, para que possam utilizá-los e partilhá-los com segurança com parceiros de confiança, com a certeza de que os dados estão protegidos, seguros e são acedidos apenas pelas pessoas que precisam deles, quando precisam, utilizando os princípios do privilégio mínimo (Rose, *et.al*, 2020).

O modelo de segurança ZT repensa como implementar o acesso de forma segura aos recursos e ativos mais importantes da organização. Ele é determinado por uma política dinâmica baseado em níveis de confiança que são construídos a partir de vários atributos do sujeito da organização a ser autenticado como: identidade, localização, hora e postura de segurança do dispositivo.

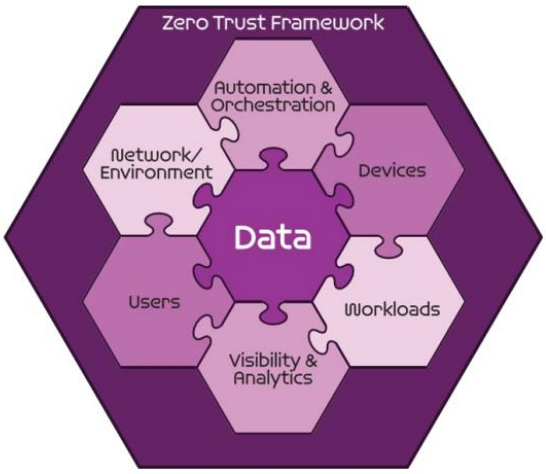
A ZT possui cinco princípios a saber na NIST 800-207 (Rose, *et.al*, 2020):

Presunção de um ambiente hostil - principio que determina que existem pessoas mal-intencionadas tanto dentro, quanto fora do ambiente. Todos os usuários, dispositivos, aplicativos, ambientes, redes OT e todos os outros são tratados com não confiáveis;

a) **Presunção de violação** - a centena de milhares de ataques todos os dias buscando a negação do serviço. Operar e defender seus recursos consciente que seu adversário já está presente no seu ambiente. Faça uma análise mais aprimorada de decisões de acesso e autorização para melhor filtragem e repostas a incidentes;
b) **Nunca Confie, sempre verifique** - negar o acesso por padrão. Cada dispositivo, usuário, aplicativo, rede de trabalho e fluxo de dados devem ser autenticados e explicitamente autorizados usando privilégios mínimos, múltiplos fatores e políticas dinâmicas de segurança cibernética;
c) **Examine exaustivamente** - Todos os recursos são acessados consistentemente de forma segura usando vários atributos (dinâmicos e estáticos) para derivar níveis de confiança para acesso contextual aos recursos; e
d) **Aplique análise unificada** – aplicar uma análise unificada dos dados, aplicativos, ativos e serviços para incluir análise comportamental e registrar cada transação.

Os pilares da ZT devem atender as necessidades da organização e podem ser identificados como um quebra-cabeça que deve ser interligado e complementar, conforme figura 4.

Figura 4: Pilares da ZT da NIST 800-207.



Fonte: Rose, *et.al*, 2021.

Os pilares da ZT trabalham juntos para proteger efetivamente o Pilar de dados, mas de acordo com o principal negócio da organização, pode ser focado na disponibilidade do sistema. Os controles previstos nos pilares são previstos na NIST 800-207 (Rose, *et.al*, 2020):

a) **Usuários** - proteger, limitar e impor o acesso as pessoas e entidades não pessoais, entidades e dados. Forte Gerenciamento de privilégio de acesso;
b) **Dispositivos** - Autenticação contínua em tempo real, inspeção, avaliação e aplicação de patches de dispositivos em uma empresa são funções críticas. Avaliações de confiança de dispositivos, determinação de autorização e limitação de acesso;
c) **Rede e ambiente** - Segmentar (tanto lógica quanto fisicamente), isole e controle a rede/ambiente (no local e fora do local) com restrições de acesso e política granulares. É essencial controlar o acesso privilegiado, gerenciar fluxos de dados internos e externos e evitar movimentação lateral;
d) **Aplicações e Balanceamento de carga** - Aplicações e o balanceamento das cargas de trabalho incluem tarefas em sistemas ou serviços no local, bem como aplicações ou serviços em execução em um ambiente de nuvem. Proteger e gerenciar adequadamente a camada de aplicação, bem como contêineres de computação e máquinas virtuais, é essencial para a ZT;
e) **Dados** - As organizações precisam categorizar seus dados em termos de criticidade da missão e usar essas informações para desenvolver uma estratégia

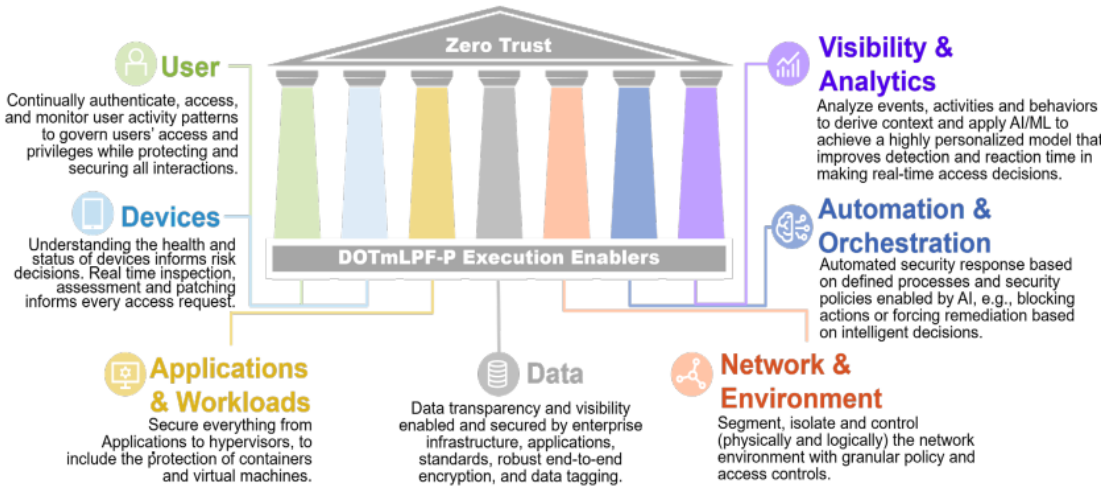
abrangente de gerenciamento de dados como parte de sua abordagem geral de ZT.

f) **Visibilidade e Análise** - Essa visibilidade melhora a detecção de comportamento anômalo e fornece a capacidade de fazer alterações dinâmicas na política de segurança e decisões de acesso em tempo real. Uma empresa ZT capturará e inspecionará o tráfego, olhando além da telemetria de rede e nos próprios pacotes para descobrir com precisão o tráfego na rede e observar as ameaças que estão presentes e orientar as defesas de forma mais inteligente; e

g) **Automação e Orquestração** - Automatizar processos de segurança manuais para tomar ações baseadas em políticas em toda a empresa com rapidez e em escala. O SOAR melhora a segurança e diminui os tempos de resposta. A orquestração de segurança integra o *Security Information and Event Management* (SIEM) e outras ferramentas de segurança automatizadas e auxilia no gerenciamento de sistemas de segurança distintos.

Ademais, a Departamento de Defesa americano (DoD) inclui os pilares com alicerces para sua estratégia de ZT para suas organizações, conforme figura 5.

Figura 5: Estratégia do DoD de ZT.



Fonte: Department of Defense EUA, 2021.

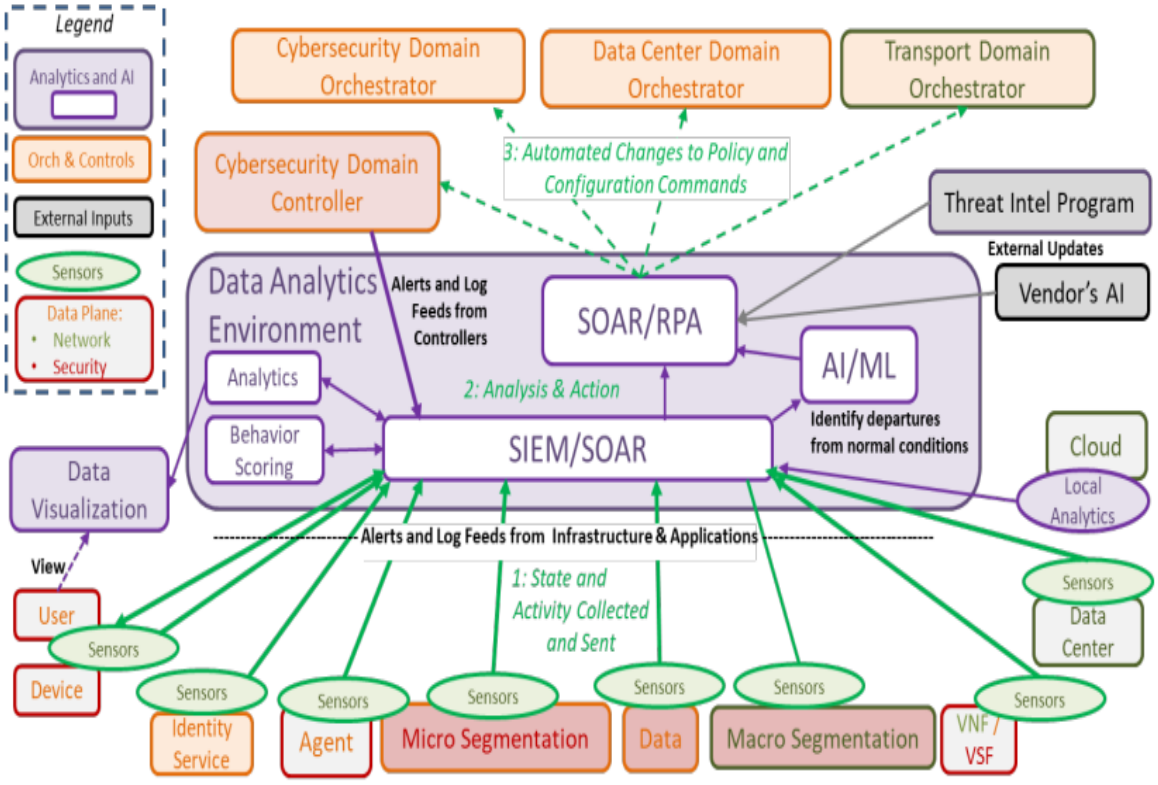
O modelo ZT deve utilizar as análises de Big Data para entender o comportamento das suas redes e dos seus dados, usuários e redes. Em um modelo de ZT com maior

maturidade podemos incluir a Inteligência Artificial (IA) para poio a decisão supervisionado (Hurel, 2021).

O Big Data Analytics e a IA dentro do ZT aumentam drasticamente a visibilidade, o insight e a automação no ambiente. Os dados são coletados centralmente de todos os aspectos do ambiente e analisados. A quantidade de dados coletados em um modelo ZT é muito maior do que a arquitetura tradicional devido aos dados necessários para alimentar a automação e, portanto, requer ferramentas mais avançadas, conforme figura 6.

Por fim, a estratégia do Departamento de Defesa americano deixou como oportunidade de melhoria para o futuro, a inclusão da ZT sendo utilizada para a Base Industrial de Defesa para os anos de 2023 até 2027. Desta forma, observa-se a utilização da ZT para as IC do EUA (United States, 2022).

Figura 6: Estratégia do DoD de ZT.



Fonte: Department of Defense EUA, 2021.

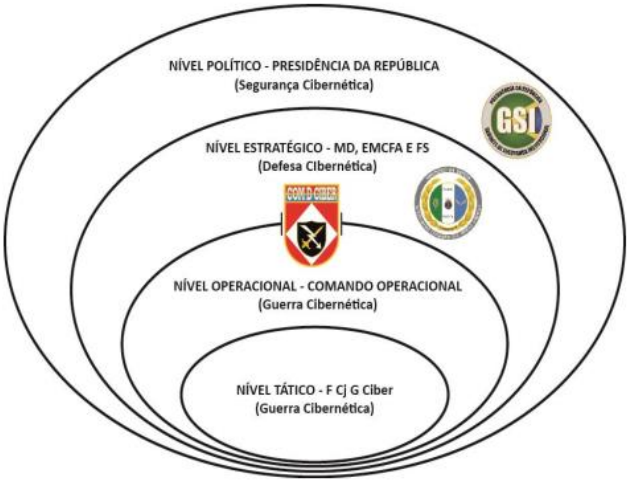
No Brasil a missão de segurança cibernética da IC é de responsabilidade do GSI/PR que pode solicitar apoio do Comando de Defesa Cibernético (ComDCiber) do Exército Brasileiro, conforme a Doutrina Militar de Defesa Cibernética (Brasil, 2023).

2.3 A segurança e defesa cibernética no Brasil.

A Estratégia Nacional de Defesa (Brasil, 2008) determinou as diversas áreas de atuação para as Forças Armadas. Dentre elas podemos citar: o setor nuclear para a Marinha do Brasil, o setor cibernético para o Exército Brasileiro e o setor aeroespacial para da Força Aérea Brasileira.

Contudo, depois da aprovação da END, três campos distintos passaram a ser reconhecidos no setor cibernético: a Segurança Cibernética, a cargo da Presidência da República (PR); a Defesa Cibernética, a cargo do Ministério da Defesa; e a Guerra Cibernética, a cargo dos Comandos Operacionais ativados e de suas Forças Componentes, conforme figura 7.

Figura 7: Níveis de decisão e atores no espaço cibernético.



Fonte: Brasil, (2023).

Podemos observar na figura 7 que o nível de decisão político é responsável pela segurança cibernética. A segurança cibernética são ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis, conforme Glossário do Gabinete de Segurança Institucional (Brasil, 2021b).

Ademais, as ações do nível político são coordenadas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), abrangendo a Administração Pública Federal (APF) e as Infraestruturas Críticas (IC).

Outrossim, o Decreto n° 11.856, de 26 de dezembro de 2023, institui a Política Nacional de Cibersegurança (Brasil, 2023a), orienta a atividade de segurança cibernética no País, tem como princípios fundamentais no seu art. 2º a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos, a prevenção de incidentes e de ataques cibernéticos, em particular aqueles dirigidos a infraestruturas críticas nacionais e a serviços essenciais prestados à sociedade e, por fim, prevê a cooperação entre órgãos e entidades, públicas e privadas, em matéria de segurança cibernética.

Desta forma, fica com um encargo que prevê inclusive a criação de Sistema Integrado de Dados de Segurança das Infraestruturas Críticas. Contudo, a ENSIC determina que:

> Em uma visão mais ampla, a atividade de segurança de infraestruturas críticas tem por finalidade articular, em diversos níveis e esferas **do Poder Público**, bem como no setor privado, o desenvolvimento de um processo de segurança preventiva de recursos humanos, de equipamentos, de instalações, de serviços, de sistemas, de informações e de outros recursos que, de alguma forma, assegurem a resiliência e o funcionamento dos serviços e das atividades indispensáveis ao Estado e à sociedade.
> Portanto, para obtenção dos melhores resultados, a colaboração no fornecimento de dados precisos sobre as infraestruturas e suas respectivas operações é de suma importância. Com essa troca de informações, o trabalho alcançará seu objetivo de promover a prevenção e a redução de riscos e custos, especialmente aqueles relativos à segurança e à **defesa da sociedade** e do Estado brasileiros.

Portanto, a ENSIC prevê que a Defesa participe efetivamente para promover a prevenção e a redução de riscos e custos para as IC. A doutrina Militar de Defesa Cibernética também aprova a criação do Sistema Militar de defesa Cibernética (SMDC), onde está previsto:

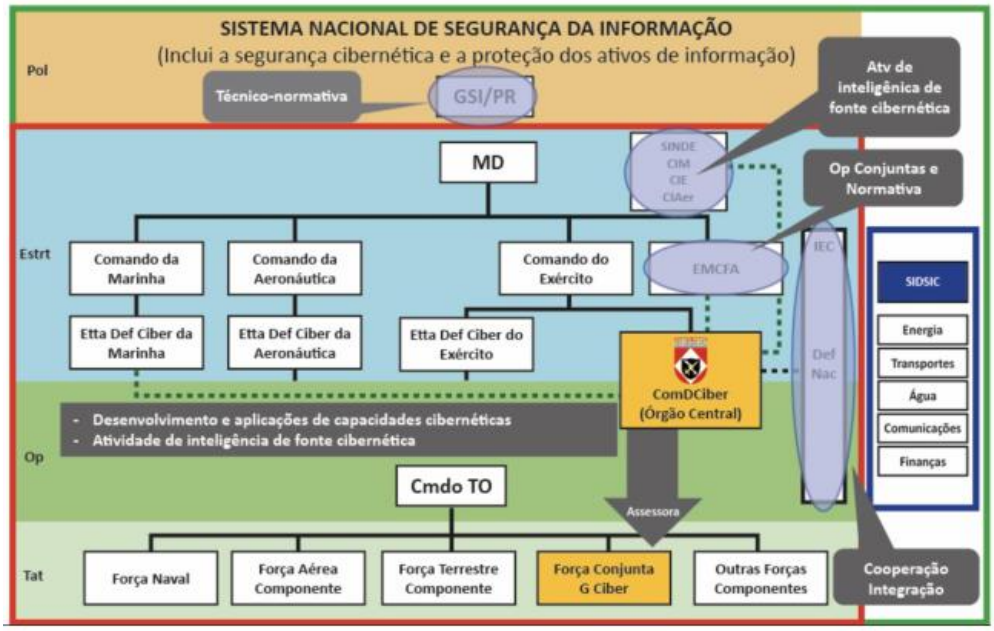
> 1.3.3 Outro fato relevante para o Sistema Militar de Defesa Cibernética (SMDC) foi a publicação do Decreto nº 9.637/2018, o qual instituiu a Política Nacional de Segurança da Informação (PNSI), incluindo a Segurança Cibernética e a Defesa Cibernética na abrangência da Segurança da Informação em âmbito nacional.
> ....
> 2.3.10 Aumento da Resiliência do espaço cibernético não pertencente ao SMDC - as Op Ciber Def geralmente focam nos ativos do SMDC. Entretanto, as ações cibernéticas podem **proteger qualquer outra porção do espaço cibernético nacional**, uma vez que as operações militares dependem de outros segmentos do espaço cibernético, **incluindo aqueles da iniciativa privada, e de outras agências governamentais**.
> 2.3.11. Quando necessário e autorizado, mediante coordenação com o GSI/PR, MD e outros ministérios e agências, as FA e o ComDCiber **contribuirão para a proteção de outras infraestruturas** críticas e recursos-chave nacionais.

Conclui-se, então, que o ComDCiber, como órgão central do SMDC quando enquadrada no nível estratégico, possui uma responsabilidade conjunta de integrar a segurança cibernética das IC em coordenação com o GSI/PR, conforme figura 8.

> 3.3.6 O ComDCiber mantém canal técnico para coordenação e integração com os órgãos de interesse envolvidos nas atividades de Defesa Cibernética (CERT.br, CTIR Gov, órgãos de Defesa/Guerra Cibernética das FA, Ministérios, Agências Governamentais, dentre outros).

Desta forma, conforme previsto no SMDC, o ComDCiber já possui uma relação estreita com órgãos da iniciativa privada (CERT.Br), dos ministérios e agências governamentais. A figura 8, ainda, mostra que o ComDCiber tem responsabilidade com as IEC, abreviatura usada no manual para IC, e o setor energético aparece em primeiro lugar para a proteção do ComDCiber.

Figura 8: Organograma do Sistema Militar de Defesa Cibernética (SMDC).



Fonte: Brasil, 2020d.

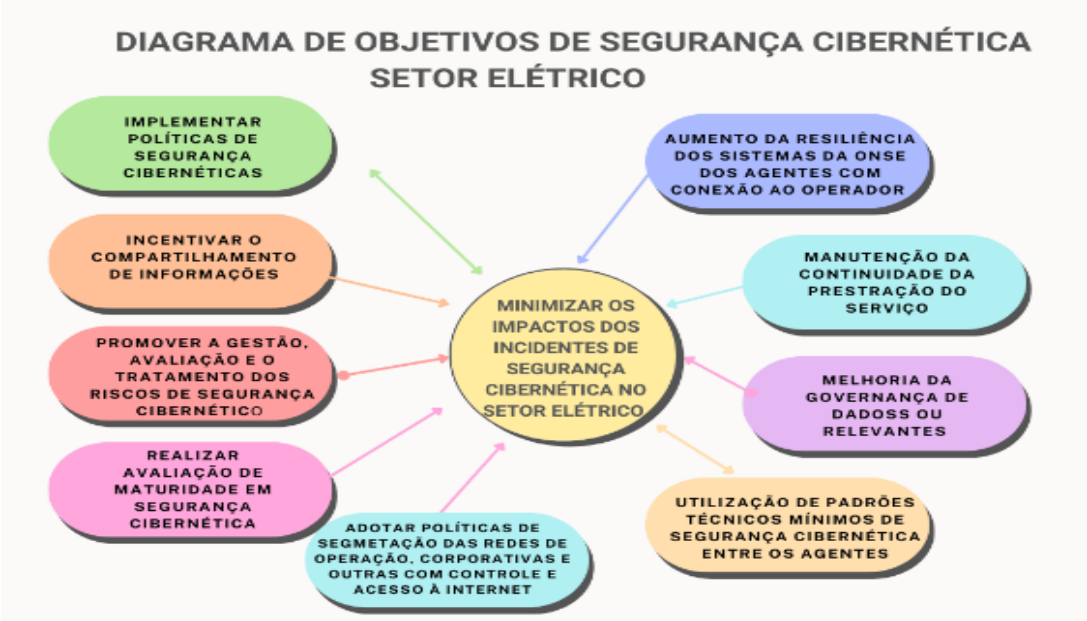
Por fim, o ComDCiber, ente da Defesa com alta capacidade técnica, conforme descrito na sua missão institucional, pode contribuir com a implementação da ZT para proteção da ONS, em coordenação com GSI/PR, com a finalidade de atender as demandas previstas na ENSIC e na Doutrina Militar de Defesa Cibernética.

2.4 Como a arquitetura ZT contribui com a segurança do setor elétrico

A Agência Nacional de Energia Elétrica (ANEEL), abriu uma consulta pública 007/2021 com o objetivo de ter contribuições para construir uma Análise de Impacto Regulatório sobre a segurança cibernética do Setor Elétrico Brasileiro, conforme figura 9.

Fica evidente a necessidade de implementar normas e diretrizes que promovam que todas as empresas da ONS adotem a arquitetura *Zero Trust*. Para isso é necessário um investimento em programas de capacitação para profissionais de TI e segurança cibernética no setor elétrico sobre os princípios e práticas do *Zero Trust*. Tal programa incluirá ações para criar um ambiente robusto de defesa cibernética que não só proteja as infraestruturas críticas do setor elétrico, mas também promova uma cultura de segurança em toda a cadeia de fornecimento de energia.

Figura 9: Diagrama de objetivos de segurança cibernética no setor elétrico.



Fonte: Adaptado do Kraemer, 2021.

Ademais, é necessário a criação de fóruns de cooperação entre diferentes agências governamentais, empresas de energia e especialistas em cibersegurança para troca de informações e melhores práticas. Para alcançar este objetivo, deve-se buscar estabelecer parcerias público-privadas que incentivem a implementação e incentivo a financiamento de tecnologias *Zero Trust* e a partilha de inteligência sobre ameaças.

Por oportuno, a eficiência da aplicação da arquitetura deverá ser avaliada através de métricas claras como teste de intrusão (*pentest*) semestrais, auditorias feitas por empresas externas e implementação de teste de *Disaster Recovery*, medindo assim, as medidas de segurança cibernéticas granulares em cada micro segmentação da rede.

Por fim, são necessários incentivos de Parcerias Públicas Privadas (PPP) para o desenvolvimento de tecnologia e produção da Base Industrial de Defesa (BID) para produção de cadeias de suprimento (*supply cha*in) de hardware e software capazes de

nos tornar as infraestruturas brasileiras independentes de tecnologias externa a nação (AMARAL, 2022).

3 CONSIDERAÇÕES FINAIS

Os Sistemas de Controle Industrial (ICS) servem como a força vital da civilização contemporânea, orquestrando as operações que fazem, movem e energizam o mundo. Neste sentido, as redes elétricas são responsáveis por iluminar, aquecer e resfriar as casas, as instalações de engenharia que tratam e fornecem água potável e segura e as fábricas que produzem os bens essenciais do País.

Esta interdependência do setor elétrico somado a grande capacidade nacional de ser uma superpotência energética, transformam o Brasil em uma párea internacional com grandes capacidades de negociação. Desta forma, a proteção de uma possível interrupção no setor elétrico é fundamental para manter as infraestruturas críticas vitais para a segurança nacional, instabilidade econômica e projeção internacional do Brasil.

No entanto, a criticidade dos ICS os torna um alvo atraente para adversários maliciosos. Ataques cibernéticos a esses sistemas podem ter consequências catastróficas, que vão desde quedas de energia generalizadas e cadeias de suprimentos interrompidas até desastres ambientais, ferimentos humanos e potencial perda de vidas.

A responsabilidade pela segurança cibernética desta IEC é do GSI/PR., Contudo, a falta de mão de obra especializada e pouco efetivo do órgão se torna uma barreira para a consecução de sua missão. Para solucionar este óbice é necessário repensar uma parceria integradora entre o Sistema Militar de Defesa Cibernética (SMDC) com o Sistema Integrado de Dados de Segurança das Infraestruturas Críticas, previsto na PNSIC.

Paralelamente, estes sistemas elétricos teriam sua cibersegurança garantida através de um novo modelo de arquitetura de redes micro segmentadas, arquitetura *Zero Trust* (ZT).

Este modelo prevê novos sistemas de autenticação baseados em pilares e princípios que garantem: todas as fontes de dados e serviços computacionais são considerados recursos, toda comunicação é protegida independente de sua localização, o acesso aos recursos individuais da organização é concedido para cada sessão, o acesso aos recursos é determinado por uma política atualizada dinamicamente, a organização monitora a integridade e segurança de todos os ativos, toda autenticação e autorização de recursos é dinâmica e estritamente aplicada antes que o acesso seja concedido e a organização coleta o máximo possível de informações sobre o estado

atual dos ativos, infraestrutura de rede e comunicações e as usa para melhorar sua política de segurança (Amaral, 2022).

Para isso, métricas claras de avaliação da arquitetura são implementadas e planos de ação para manter a resiliência cibernética farão parte do arcabouço da ZT. Ainda, a arquitetura contará com o incentivo do desenvolvimento de soluções inovadoras que possam ser integradas a mesma como: inteligência artificial e machine learning para monitoramento de segurança e busca avançada de inteligência cibernética.

Por fim, pode -se concluir que a ZT pode ser uma solução para a cibersegurança das IEC do setor energético de Brasil e que, quer em tempo de paz ou de guerra, é necessário pensar como garantir o pleno funcionamento desta IEC tão importante dentro do cenário brasileiro e global.

REFERÊNCIAS

AMARAL, THIAGO M. S. (2022). **Proposta de integração de controles de segurança baseados nos princípios Zero Trust em uma cyber supply chain**. Dissertação de Mestrado Profissional, Publicação PPEE.MP.030, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 76 p.

ALAGAPPAN, Annamalai: VENKATACHARY, Sampath Kumar: ANDREWS, L.J. Baptist. "**Augmenting Zero Trust Network Architecture to Enhance Security in Virtual Power Plants**." *Energy Reports*, vol. 8, Nov. 2022, pp. 1309–1320, Disponível em: https://doi.org/10.1016/j.egyr.2021.11.272. Acesso em: 20 set. 2024.

ATAQUES cibernéticos crescem no setor elétrico, mas risco à usina nuclear é baixo. **Isto É Dinheiro**, 4 fev. 2021. Disponível em: https://istoedinheiro.com.br/ataques-ciberneticos-crescem-no-setor-eletrico-mas-risco-a-usina-nuclear-e-baixo-2/. Acesso em: 20 set. 2024.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Promulgada em 5 de outubro de 1988. Brasília, DF: Presidência da República, [2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.html. Acesso em: 20 set. 2024.

BRASIL. **Decreto n° 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF: PR, 2020e. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 20 set. 2024.

BRASIL. **Decreto n° 10.569, de 9 de dezembro de 2020**. Aprova a Estratégia Nacional de Segurança das Infraestrturas Críticas (ENSIC). Brasília, DF: PR, 2020e. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm. Acesso em: 20 set. 2024.

BRASIL. **Decreto n° 11.331, de 1° de janeiro de 2023.** Aprova a Estrutura Regimental do Gabinete de Segurança Institucional da Presidência da República. Brasília, DF: PR, 2023a. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11676.htm#art5. Acesso em: 20 set. 2024.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa. Política Nacional de Defesa**. Brasília, DF: MD, 2020a. Versão sob apreciação do Congresso Nacional (Lei Complementar 97/1999, art. 9º, § 3º). Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-edefesa/pnd_end_congresso_.pdf. Acesso em: 20 set. 2024.

BRASIL. Ministério da Defesa. **Glossário das Forças Armadas: MD35-G-01**. 5. ed. Brasília, DF: MD, 2015. 288 p. Disponível em: https://www.gov.br/defesa/ptbr/arquivos/legislacao/emcfa/publicacoes/doutrina/

md35-G-01-glossario-das-forcasarmadas-5-ed-2015-com-alteracoes.pdf/view. Acesso em: 20 set. 2024.

BRASIL. Ministério da Defesa. **Portaria nº 3.781 de 17 de novembro de 2020**. Cria o Sistema Militar de Defesa Cibernética (SMDC) e dá outras providências. Brasília, DF: MD, 2020d. Disponível em: https://www.in.gov.br/web/dou/-/portaria-n-3.781/gm-md-de-17-de-novembro-de-2020-289248860. Acesso em: 20 set. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Glossário de Segurança da Informação**. Brasília, DF: GSI, 2021b. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370. Acesso em: 20 set. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Portaria nº 120, de 21 de dezembro de 2022**. Aprova o Plano de Gestão de Incidentes Cibernéticos para a administração pública federal. Brasília, DF: GSI, 2022b. Disponível em: https://in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918. Acesso em: 20 set. 2024.

BRASIL. Ministério da Defesa. **MD31-M-07**: Doutrina Militar de Defesa Cibernética. Brasília, DF: MD, 2023.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. **Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)**. Cyber-attack against Ukrainian critical infrastructure. [*S. l.*]: CISA, 2021. Disponível em: https://bit.ly/3psT1Sx. Acesso em: 20 set. 2024.

CYBER SECURITY COALITION. **Cyber security incident management guid**e. Brussels: Cyber Security Coalition, 2016. Disponível em: <https://cybersecuritycoalition.be/wp-content/uploads/cybersecurity-incident-management-guide_EN.pdf>. Acessado em: 16 set. 2024.

CISO ADVISOR. **Ataque a distribuidora de energia destrói 25 anos de dado**s. [S. l.]: CISO Advisor, 2021. Disponível em: https://bit.ly/3T1c83v. Acessado em: 20 set. 2024.

DE CONTEÚDO PARA DOCENTES, G. **Cibersegurança e Ética de Dados no Setor Elétrico**. Disponível em:https://www.gov.br/mec/pt-br/areas-de-atuacao/ept/profissionais-futuro/Ciberseguranca__1_2.pdf>. Acessado em: 23 set. 2024.

FEDERICI, F.; MARTINTONI, D.; SENNI, V. **A zero-trust architecture for remote access in industrial IoT infrastructures. Electronics**, v. 12, n. 3, p. 566, 2023.

GÓES, Guilherme Sandoval. Grande Estratégia Brasileira da Tríplice Tríade: pensando o futuro do País. **Revista da Escola Superior de Guerra**, Rio de Janeiro, v. 39, n. 86, p. 34–61, 2024.

HUREL, Louise Marie. **Cibersegurança no Brasil**: uma análise da estratégia nacional. Rio de Janeiro: Instituto Igarapé, 2021. Disponível em:

https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf . Acesso em: 20 set. 2024.

JE, Donghyun; JUNG, Jungsoo; CHOI, Sunghyun. Toward 6G security: technology trends, threats, and solutions. **IEEE Commun. Standards Mag**., v. 5, n. 3, p. 64–71, Sept. 2021.

KRAEMER, Rodrigo Antonio S.; IZUMIDA, Marcos. Brasília, DF: MEC, 2023. **Cibersegurança e ética de dados no setor elétrico**. Disponível em: https://www.gov.br/mec/pt-br/areas-de-atuacao/ept/profissionais-futuro/Ciberseguranca__1_2.pdf. Acesso em: 23 set. 2024.

IRONNET THREAT RESEARCH TEAM; DEMBOSKI, M. **Industroyer2 malware targeting Ukrainian energy company.** Washington, DC: IronNet, 2022. Disponível em: https://www.ironnet.com/blog/industroyer2-malware-targeting-ukrainian-energy-company. Acesso em: 20 set. 2024.

RAMEZANPOUR, K.; JAGANNATH, J. **Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN**. Computer networks, v. 217, n. 109358, p. 109358, 2022.

ROSE, Scott et al. NIST special publication 800-207 zero trust architecture. **NIST National Institute of Standards and Technology US Department of Commerce**, p. 800-207, 2020.

UNITED STATES. Department of Defense. **Zero Trust Reference Architecture Version 2.0.** Washington, DC: DOD, 2022. Disponível em: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf. Acessado em: 20 set. 2024.