GESEL

Grupo de Estudos do Setor Elétrico

UFRJ

Segurança Cibernética do Setor Elétrico Brasileiro: Desafios Regulatórios e Tecnológicos

Iony Patriota de Siqueira
Nivalde de Castro
Mauricio Moszkowicz
Lorrane Câmara

TDSE

Texto de Discussão do Setor Elétrico

Nº 103

agosto de 2021
Rio de Janeiro

GESEL
Grupo de Estudos do Setor Elétrico
UFRJ

TDSE

Texto de Discussão do Setor Elétrico Nº 103

Segurança Cibernética do Setor Elétrico Brasileiro: Desafios Regulatórios e Tecnológicos

Iony Patriota de Siqueira
Nivalde de Castro
Mauricio Moszkowicz
Lorrane Câmara

ISBN: 978-65-86614-28-2

agosto de 2021

Sumário

Lista de Figuras

Lista de Tabelas

Abreviaturas

ABEEOLICA	Associação Brasileira de Energia Eólica
ABNT	Associação Brasileira de Normas Técnicas
ANA	Agência Nacional de Águas
ANEEL	Agência Nacional de Energia Elétrica
ANP	Agência Nacional do Petróleo Gás Natural e Biocombustíveis
CA	Corrente Alternada
CAG	Controle Automático de Geração
CC	Corrente Contínua
CDCiber	Centro de Defesa Cibernética do Exército Brasileiro
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
CIGRE	*International Council on Large Electric Systems*
CIS	*Center for Internet Security*
CITDigital	Comitê Interministerial para a Transformação Digital
CMM	*Capability Maturity Model*
CMSE	Comitê de Monitoramento do Setor Elétrico
COBIT	*Control Objectives for Information and Related Technology*
CSIRT	*Computer Security Incident Response Team*
CTIR	Centro de Tratamento a Incidentes em Redes de Computadores
CTIRGov	Centro de Tratamento e Resposta a Incidentes Cibernéticos do Governo
DCS	*Distributed Control Systems*
DER	*Distributed Energy Resource*
DERMS	*Distributed Energy Resource Management System*

DG	*Distributed Generation*
DMZ	*Demilitarized Zone*
DR	*Demand Response*
DSO	*Distribution System Operator*
EB	Exército Brasileiro
E-Ciber	Estratégia Nacional de Segurança Cibernética
E-Digital	Estratégia Brasileira para a Transformação Digital
EMS	*Energy Management System*
ENSIC	Estratégia Nacional de Segurança de Infraestruturas Críticas
GCSCC	*Global Cyber Security Capacity Centre*
GSI	Gabinete de Segurança Institucional
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronic Engineers*
IoT	*Internet of Things*
ISA	*International Society of Automation*
ISO	*International Standards Organization, Independent System Operator*
ITU	*International Telecommunication Union*
LAN	Local Area Network
LGPD	Lei Geral de Proteção de Dados
MD	Ministério da Defesa
NERC	*North American Electric Reliability Corporation*
NIC	Núcleo de Informação e Coordenação
NIST	*National Institute of Standards and Technology*
OAS	*Organization of American States*
OEA	Organização dos Estados Americanos
ONS	Operador Nacional do Sistema Elétrico

PERA	*Purdue Enterprise Reference Architecture*
PLC	*Programmable Logic Controllers*
PMU	*Phasor Measuring Unit*
PNSI	Política Nacional de Segurança da Informação
PNSIC	Política Nacional de Segurança de Infraestruturas Críticas
PR	Procedimentos de Rede, Presidência da República
PV	*Photo-Voltaic*
QoS	Qualidade de Serviço
RBAC	*Role-based Access Control*
RED	Recurso Energético Distribuído
SCADA	*Supervisory Control and Data Acquisition*
SEB	Setor Elétrico Brasileiro
SEP	Sistemas Especiais de Proteção
SGRED	Sistema de Gerenciamento de Recursos Energéticos Distribuídos
SIN	Sistema Interligado Nacional
SinDigital	Sistema Nacional para a Transformação Digital
TI	Tecnologia de Informação
TL	Tecnologia de Telecomunicações
TO	Tecnologia de Operação
TSO	*Transmission System Operator*
VPN	*Virtual Private Network*
VPP	*Virtual Power Plant*

1. Introdução

Em todo o mundo, proliferam os casos de ataques cibernéticos às infraestruturas críticas nacionais, em particular às redes de energia elétrica. Como rede sociotécnica catalizadora de muitos outros domínios da sociedade, o setor elétrico destaca-se não apenas por sua vulnerabilidade e exposição, mas principalmente pela extensão dos possíveis danos que ataques cibernéticos podem causar, amplificados pela capilaridade com outros setores críticos da sociedade.

Simultaneamente, a automação e a digitalização das redes elétricas e dos demais setores de infraestruturas críticas e o intenso uso de meios de comunicação para sua operação e gestão aumentam as superfícies de ataque com as vulnerabilidades próprias destes domínios.

Neste contexto, o presente texto utiliza uma abordagem estruturada para realizar um levantamento situacional da Segurança Cibernética do Setor Elétrico Brasileiro e do fornecimento de energia no país.

Uma abordagem de cima para baixo (*topdown*) será utilizada, com início na definição das estratégias de transformação digital na administração pública brasileira, incluindo a proteção de infraestruturas críticas e da informação em geral, com ênfase na regulamentação, nas políticas públicas, na governança e nos controles aplicáveis aos setores produtivos nacionais e aos cidadãos de maneira geral.

Em seguida, esta análise será particularizada para o setor elétrico como uma das principais infraestruturas críticas do país, descrevendo sua arquitetura e o arcabouço regulatório da segurança cibernética, com proposições de regulamentações para discussão.

O restante deste texto está estruturado nos seguintes capítulos. O Capítulo 2 introduz a estrutura organizacional e funcional do Setor Elétrico Brasileiro (SEB), como preâmbulo à análise da segurança cibernética.

A abordagem será baseada em uma arquitetura hierárquica de camadas, modelando a estrutura vertical do setor, que inclui a geração, a transmissão, a distribuição e o consumo de energia elétrica pela sociedade, e interligando todos os domínios de segurança, desde o nível físico das instalações até a operação do Sistema Interligado Nacional (SIN). Ênfase será dada à interdependência do setor elétrico com as demais redes de infraestruturas críticas, a nível nacional e internacional.

O Capítulo 3 avalia a segurança cibernética no Brasil sob o aspecto regulatório, com destaque às estratégias de transformação digital e de segurança cibernética adotadas, às políticas, estratégias e diretrizes aplicadas aos órgãos de administração federal e às redes de infraestruturas críticas, dentre as quais o sistema elétrico nacional. Ênfases serão dadas à estrutura organizacional e de governança, bem como aos sistemas de controle existentes [7].

O Capítulo 4 aprofunda a análise da segurança dos setores de infraestruturas críticas, especialmente do SIN, objetivando a proposição de aspectos regulatórios necessários para o futuro. Três campos tecnológicos serão vitais neste contexto, de particular interesse para o setor elétrico, relacionados às Tecnologias Operacional (TO), Informática (TI) e de Telecomunicações (TL) [1] utilizadas em larga escala nesses setores. Uma hierarquia de definições regulatórias é desenvolvida como proposta de uma agenda regulatória para o SEB, partindo das definições de estratégias nacionais e passando pela análise de risco cibernético, pela definição de políticas, pela seleção de controles e pelas implementações tecnológicas.

No Capítulo 5, serão avaliadas as decisões regulatórias e tecnológicas aplicáveis para cada domínio e camada hierárquica do SEB, encerrando com a identificação de possíveis melhorias regulatórias.

A abordagem modela a arquitetura tecnológica, de governança e cibernética do setor elétrico, bem como sua exposição a ataques, de forma hierárquica, iniciando pelas redes nacionais e redes corporativas e passando pelos centros de controle nacionais,

regionais e corporativos, até as subestações, usinas e processos tecnológicos internos aos agentes do setor. Os diversos domínios desta arquitetura são avaliados quanto à segurança cibernética, incluindo o domínio nacional, o corporativo, o de negócios e o de operações críticas e culminando com propostas de uma abordagem integrada às definições regulatórias necessárias ao SEB.

O Capítulo final apresenta as conclusões e sugestões referentes aos aspectos tecnológicos e regulatórios mínimos a serem implementados para aperfeiçoar a segurança cibernética do Setor Elétrico Brasileiro.

2. Setor Elétrico Brasileiro

Entre as infraestruturas críticas de uma nação, o sistema elétrico desempenha um papel catalizador ao transmitir e distribuir um insumo essencial aos demais setores de infraestrutura. Simultaneamente, o setor elétrico depende de outros setores para o fornecimento de insumos energéticos (água, óleo, gás, diesel, carvão, etc.), além de informações e meios de comunicação, finanças e outros. Assim, a segurança cibernética do setor elétrico depende não apenas de sua exposição própria aos ataques, mas de sua extensão e integração continental, bem como interdependência com os demais setores críticos.

Para uma análise de sua segurança, será importante caracterizar a estrutura do SIN como uma rede elétrica única de abrangência nacional, com governança técnica centralizada no Operador Nacional do Sistema Elétrico (ONS), a estrutura operacional dos diversos agentes do setor elétrico e as características técnicas das subestações e das usinas de geração. Conjuntamente, estes elementos contribuem para o grau de exposição do setor elétrico e da superfície de ataques cibernéticos, servindo para determinar a extensão das medidas de proteção existentes e necessárias a cada nível.

As subseções seguintes resumem as características técnicas e regulatórias das redes de infraestruturas críticas e o papel do Setor Elétrico Brasileiro, em particular do SIN, em relação aos demais setores sociotécnicos nacionais. Descreve-se, também, a atuação do ONS, no topo da estrutura de governança da operação do SIN, como propositor de políticas e mecanismos regulatórios de segurança aplicáveis aos agentes do setor e às instalações elétricas.

2.1 Redes de Infraestruturas Críticas

As infraestruturas críticas de uma nação incluem os setores, as instalações, os serviços, os bens e os sistemas que, se forem interrompidos ou destruídos, provocarão sérios impactos social, econômico, político, internacional ou à segurança do Estado e da sociedade [1][8]. A segurança das infraestruturas críticas passou a ser uma tendência mundial após os atentados terroristas ocorridos nos Estados Unidos da América, em 11 de setembro de 2001.

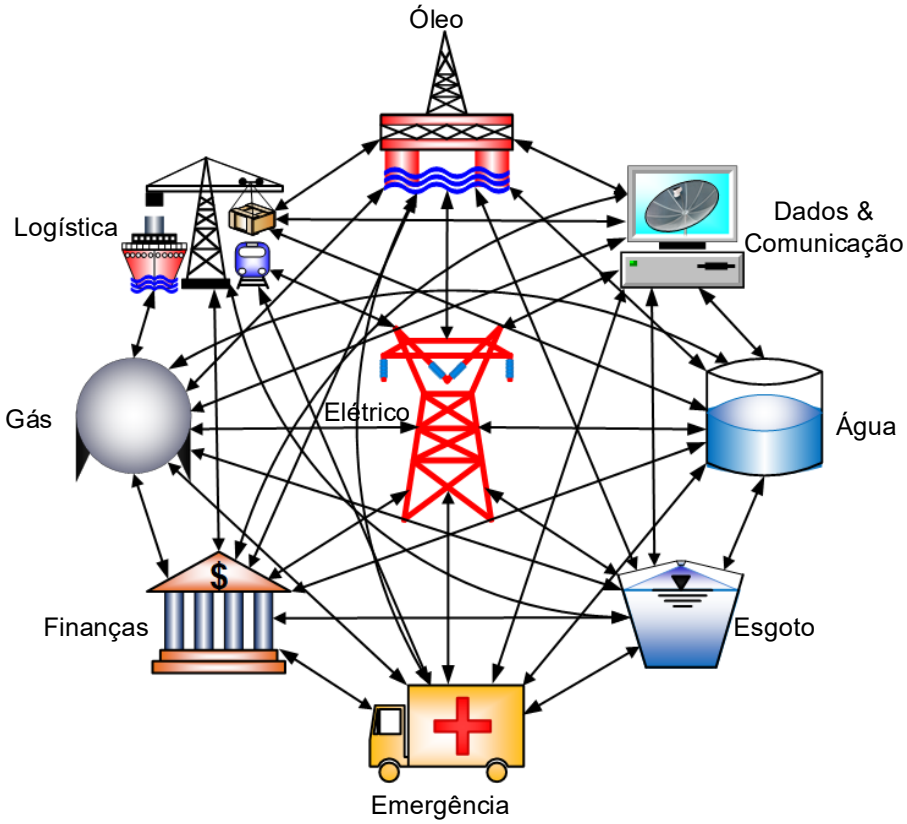
No Brasil, esta tendência teve impulso a partir de 2006, em consequência aos ataques perpetrados por uma organização criminosa a várias instalações no Estado de São Paulo [16], levando o governo brasileiro a identificar quais infraestruturas do país deveriam ser prioritariamente protegidas, no caso de novas ocorrências daquela natureza. Em consequência, as infraestruturas críticas brasileiras incluem, principalmente, os setores de comunicações, energia, transportes, finanças e águas, para os quais foram criados os Grupos Técnicos de Segurança de Infraestruturas Críticas, através do Decreto nº 9.668/2019 [17].

A estes grupos, foram solicitadas propostas para [17] "*manter em contínuo aperfeiçoamento a identificação e a classificação das infraestruturas críticas; identificar as possíveis ameaças e vulnerabilidades dessas infraestruturas críticas; e propor medidas de controle para redução dos riscos às infraestruturas críticas correspondentes à área prioritária considerada.*" Por atenderem a necessidades sociais, a segurança destas infraestruturas inclui e extrapola o âmbito de ação das próprias organizações responsáveis, exigindo a adoção de políticas públicas que preservem a segurança social.

A interdependência entre as infraestruturas críticas é um fator determinante para a segurança cibernética nacional, principalmente pela relação de dependência ou interferência de uma em outra ou de uma área prioritária de infraestruturas críticas em outra, em particular quando provocadas por ataques cibernéticos. Destaca-se que esta interdependência possui um efeito catalizador e amplificador das consequências de um incidente ou ataque em qualquer rede de infraestruturas críticas. A Figura 1 ilustra as possíveis interdependências entre os setores sociotécnicos de água, gás, óleo,

esgoto, logística, comunicação, finanças, saneamento, dados e emergência e a centralidade do setor elétrico, como catalizador destas funcionalidades, fornecendo energia para o seu funcionamento e, simultaneamente, dependendo do suporte desses setores para o seu próprio funcionamento.

Figura 1 – Centralidade do Setor Elétrico nas Infraestruturas Críticas

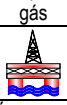


Fonte: SIQUEIRA, 2013.

Eventos e falhas em um destes setores podem ser propagados aos demais, dependendo das relações de interdependência. A Tabela 1 apresenta algumas das interdependências entre estes setores, através das funções e dos insumos demandados de cada um pelos demais, bem como os produtos e as funções fornecidos por cada um para os demais.

Destaque-se a extrema dependência na atualidade entre os setores de água, energia, óleo, gás, dados e telecomunicações, em razão da diversificação das fontes energéticas, assim como da automação e digitalização das instalações elétricas.

Tabela 1 – Interdependência entre Setores de Infraestruturas Críticas

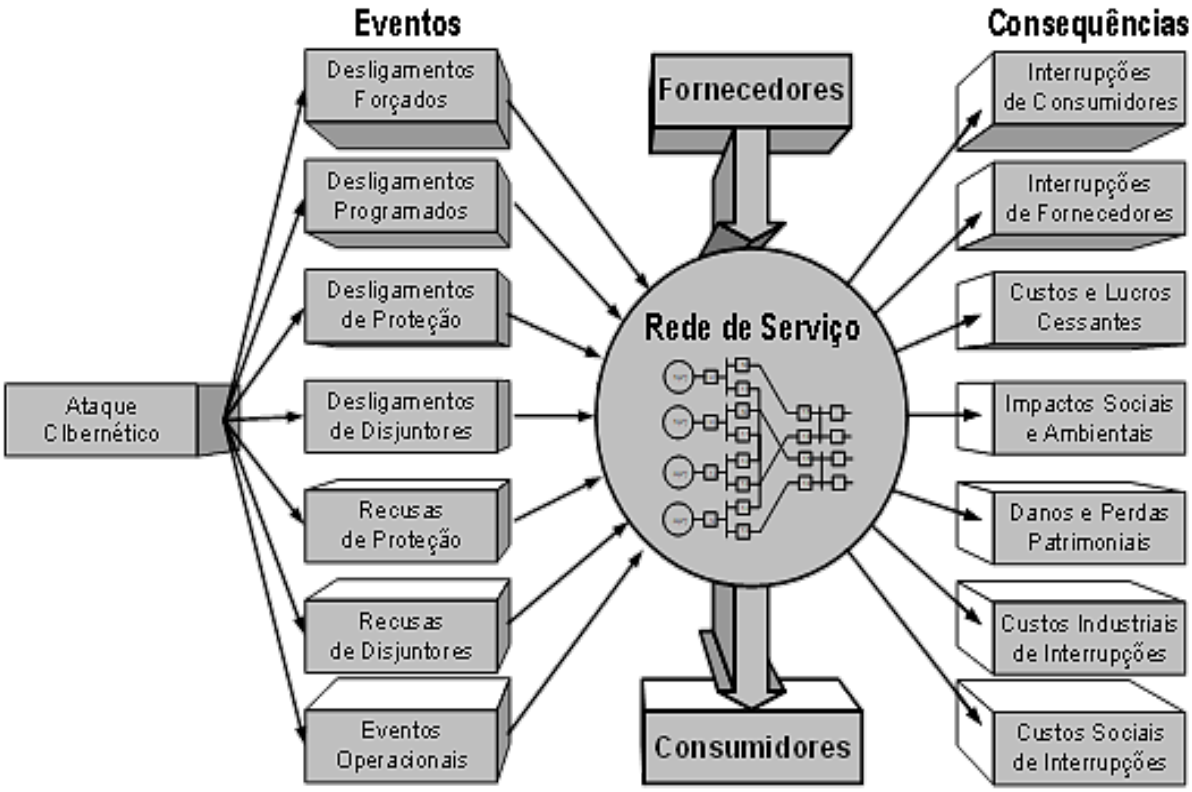
REDE	Energia	Água	Gás	Óleo	Dados	Finanças	Esgoto	Logística	Emergência
Energia		Água para resfriamento e vapor	Gás para gerar energia	Óleo para gerar energia	Dados para controle da rede	Recursos para geração e transmissão	Inundação de estação elétrica	Transporte de combustível	Socorro para falta de energia e acidente
Água	Energia para bombear e filtrar água		Gás para aquecer água	Óleo para aquecer água	Dados para controle da rede	Recursos para captação e distribuição	Infiltração de estação de água	Transporte de água	Socorro para falta de água e vazamento
Gás	Energia para comprimir e filtrar gás	Água para resfriamento e vapor		Óleo para transportar gás	Dados para controle da rede	Recursos para produção e distribuição	Inundação de estação de gás	Transporte de gás	Socorro para falta de gás e vazamento
Óleo	Energia para bombear e separar óleo	Água para resfriamento e vapor	Gás para transportar óleo		Dados para controle da rede	Recursos para produção e distribuição	Inundação de estação de óleo	Transporte de óleo	Socorro para falta de óleo e vazamento
Dados	Energia para processar dados	Água para resfriamento de centros	Gás para gerador de emergência	Óleo para gerador de emergência		Recursos para processar dados	Inundação de centro de dados	Transporte de dados	Socorro para perda de dados e suprimentos
Finanças	Energia para indústria e comércio	Água para indústria e comércio	Gás para indústria e comércio	Óleo para indústria e comércio	Dados para gestão de negócios		Inundação de centro industrial	Transporte de recursos financeiros	Socorro para assalto, incêndio e sinistro
Esgoto	Energia para bombear resíduos	Água para limpeza sanitária	Gás para bomba de emergência	Óleo para bomba de emergência	Dados para controle da rede	Recursos para saneamento urbano		Transporte de resíduos e dejetos	Socorro para entupimento e vazamento
Logística	Energia para transporte e estocagem	Água para limpeza e resfriamento	Gás para transporte e resfriamento	Óleo para transporte e resfriamento	Dados para gestão de estoques	Recursos para transporte e armazenagem	Inundação de rota ou armazém		Socorro para rota logística interrompida
Emergência	Energia para postos emergenciais	Água para posto de emergência	Gás para posto de emergência	Óleo para posto de emergência	Dados para controle de urgências	Recursos para postos emergenciais	Inundação de posto	Transporte de urgência e emergência	

Fonte: SIQUEIRA, 2013.

A Figura 2, abaixo, representa a estrutura básica da rede de um sistema sociotécnico crítico e sua relação com eventos que impactam o seu desempenho e consequências associadas.

A rede é constituída por um conjunto de ativos interligados, alimentados por fornecedores e suprindo um grupo de consumidores, representados na parte central da figura.

Figura 2 – Avaliação de Desempenho e Risco



Fonte: Adaptado de SIQUEIRA, 2013.

Diversos tipos de ataques cibernéticos podem provocar eventos imprevistos em redes sociotécnicas. Entre os principais tipos citam-se:

- Sniffer - Análise de tráfego não autorizada
- Replay – Repetição não autorizada do tráfego capturado
- Spoof – Personificação de um usuário autorizado
- DoS - Negação serviço ou sobrecarga de rede
- Erro - Erros de operadores
- Social - Engenharia social de usuários autorizados
- Vírus - Infecção por vírus de componentes do sistema
- Destruição - Destruição de dados de controle/negócios/configuração
- Modificação - Modificação de dados de controle/negócios/configuração

- Desvio - Desvio de funções e mecanismos de segurança do sistema
- Físico - Comprometimento dos mecanismos de segurança física
- Natural - Atos da natureza causando indisponibilidade do sistema

Um ataque cibernético a uma rede sociotécnica, tal como o Sistema Interligado Nacional, poderá deflagrar eventos de desligamentos forçados de disjuntores, de proteção ou programados, bem como de recusas de proteção e disjuntores, ou induzir eventos operacionais imprevistos no próprio setor ou nos setores interdependentes. As principais ameaças contra infraestruturas sociotécnicas críticas são os ataques de *phishing*, a negação de serviço em larga escala, os vazamentos de informações privadas ou institucionais, a espionagem cibernética e a interrupção de serviços.

A tendência de aplicação generalizada de dispositivos de IoT nas redes sociotécnicas e de infraestruturas críticas amplifica o espaço de exposição a ataques e representa um desafio para estas infraestruturas, tendo em vista as necessidades de equilíbrio entre segurança e privacidade e de introdução de inovações. Como consequências destes ataques, citam-se as interrupções de serviços aos consumidores e fornecedores da rede, a ampliação de custos e da necessidade de reparação de lucros cessantes, impactos sociais e ambientais, danos e perdas patrimoniais, assim como custos sociais e industriais de interrupções.

Em situação normal, nas redes sociotécnicas, excetuando-se as perdas dos processos internos, haverá um balanceamento entre o fornecimento do serviço e o seu consumo com a rede de infraestrutura operando em um estado estável [1]. Ademais, em condições normais, apenas mudanças oriundas nos mercados de fornecimento e transmissão e decisões rotineiras de natureza econômica afetarão o desempenho operacional da rede sociotécnica.

Situações anormais, por sua vez, geralmente conduzem o sistema a um estado inseguro ou instável, decorrente de fatores externos e internos, fora do controle do operador da rede. Entre os fatores mais comuns citam-se os desligamentos forçados

dos componentes por falhas internas ou erros operacionais, os desligamentos programados para manutenção ou causas operacionais, os desligamentos indevidos provocados por sistemas de proteção, os desligamentos intempestivos de seccionadores, as recusas de atuação de sistemas de proteção e seccionadores quando solicitados e eventos operacionais em geral. Estes fatores encontram-se representados no lado esquerdo da Figura 2, acima.

Diversas consequências resultam destes fatores imprevistos. Entre os mais importantes, de interesse para avaliação de desempenho e risco da rede de infraestrutura, constam as interrupções no fornecimento de serviço aos consumidores, parceiros e clientes, as interrupções do fornecimento do serviço contratado, os lucros cessantes empresariais, as perdas patrimoniais e de investimentos, as perdas de produção industrial e os custos sociais relacionados [1]. Consequências similares podem ser listadas para todos os tipos de redes de infraestrutura, conforme representadas no lado direito da Figura 2, contextualizando os objetivos desta pesquisa.

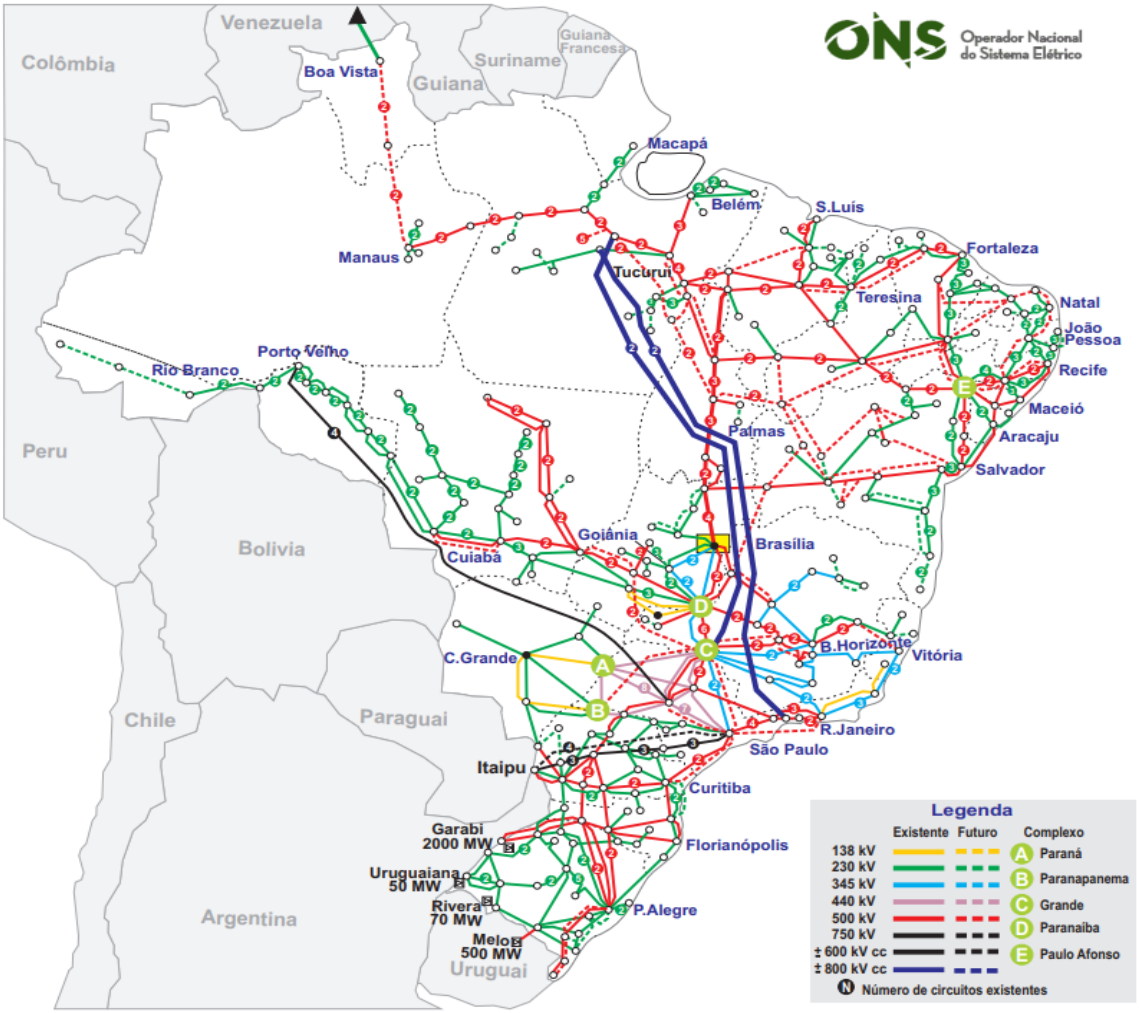
2.2 Sistema Interligado Nacional

A rede elétrica brasileira, denominada de Sistema Interligado Nacional, constitui-se de uma extensa malha de linhas de transmissão, interligando subestações e usinas localizadas em todas as regiões geográficas do país (Sul, Sudeste/Centro-Oeste, Nordeste e a maior parte da Região Norte), conforme apresentado na Figura 3, e caracteriza-se como um sistema hidro-termo-eólico de grande porte, com predominância de usinas hidroelétricas.

Por sua abrangência geográfica, comparável à da Europa continental, o SIN representa uma das mais extensas e complexas redes elétricas do mundo, operada em uma única frequência (60Hz), sob o comando de um único Operador de Sistema Independente

(ISO - *Independent System Operator*), o ONS. Esta unicidade determina simultaneamente sua grandeza, mas também sua fragilidade a ataques cibernéticos, possíveis de desativar grande parte da estrutura energética do país se não for adequadamente protegida.

Figura 3 – Mapa do Sistema de Transmissão - Horizonte 2024

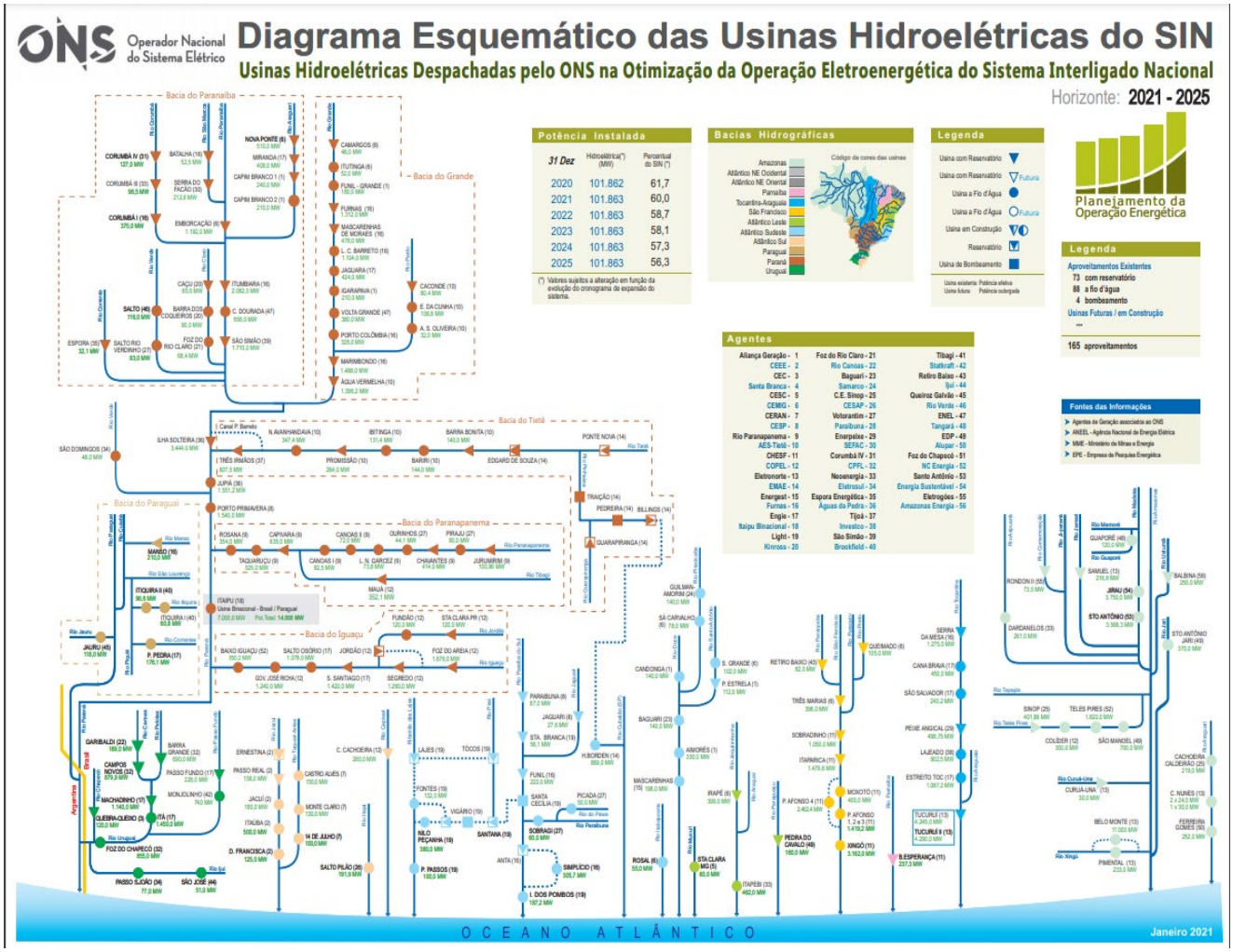


Fonte: ONS, 2021.

Como principal fonte de insumo para o setor elétrico, a rede hídrica de rios e reservatórios que alimenta as usinas hidroelétricas também forma uma extensa malha interconectada, intrinsicamente ligada à rede elétrica, cobrindo praticamente todo o território nacional (Figura 4) e com conexões internacionais.

Cada ponto desta rede representa uma interface vital para o setor elétrico, cuja interrupção provoca a suspensão de um insumo que alimenta a geração hidroelétrica e pode se propagar como efeito cascata, afetando até os consumidores de energia distantes do ponto de origem.

Figura 4 - Diagrama Esquemático das Usinas Hidroelétricas do SIN



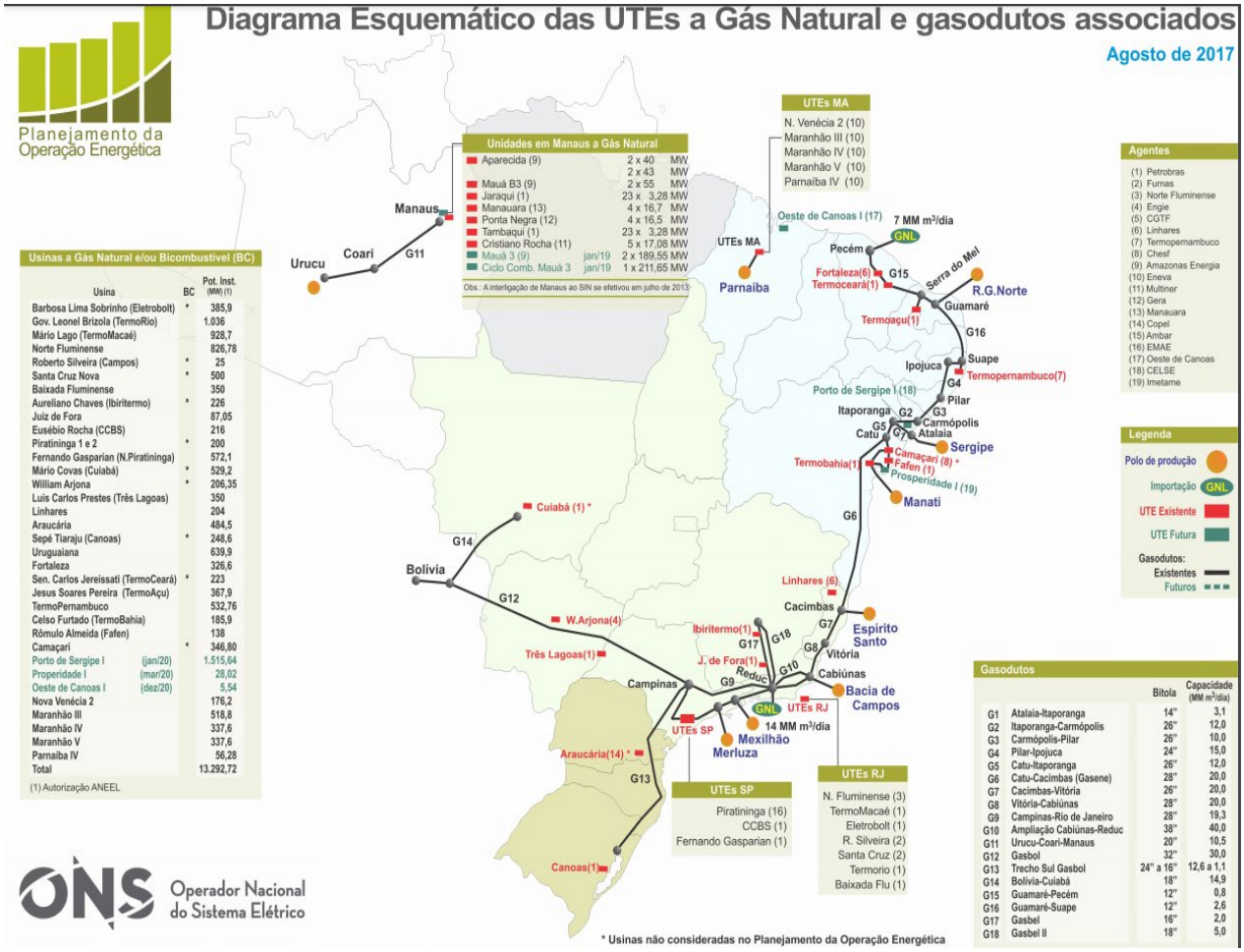
Fonte: ONS, 2021.

Localizadas nas proximidades dos principais centros de carga, as usinas térmicas contribuem para a segurança energética do SIN, sendo despachadas, atualmente, em função das condições hidrológicas das bacias hidrográficas.

Como fonte adicional de insumo para o setor elétrico, a rede de gasodutos que interliga e alimenta as usinas térmicas a gás natural também forma uma extensa malha interconectada, intrinsicamente ligada à rede elétrica, cobrindo praticamente toda a região litorânea do território nacional (Figura 5) e com conexões internacionais.

Cada ponto desta rede se interliga funcionalmente com o setor elétrico, criando uma interdependência entre estes setores energéticos críticos. Sua interrupção também resulta na suspensão de um insumo para a geração termoelétrica, podendo deflagrar um efeito cascata, de modo a impactar, inclusive, os consumidores de energia distantes do ponto de origem da falha.

Figura 5 – Rede de Termelétricas e Gasodutos a Gás Natural



Fonte: ONS, 2021.

A extensão e a interdependência destes três setores (elétrico, hidráulico e térmico) ilustram a complexidade e a vulnerabilidade do SIN a incidentes cibernéticos que possam afetar qualquer um dos seus componentes. Adicione-se a isto a crescente penetração dos Recursos Energéticos Distribuídos, liderados pela energia eólica, com participação próxima a 18 GW na matriz elétrica nacional e responsável por quase 10% nas fontes energéticas atuais, segundo a Associação Brasileira de Energia Eólica [14].

Por sua volatilidade e intermitência, situando-se fora da observabilidade e do monitoramento direto do ONS, os Recursos Energéticos Distribuídos ampliam a vulnerabilidade do SIN a ataques cibernéticos, ao agregar um grande volume de novos agentes, inclusive os de origem solar de pequeno porte, à complexa estrutura da rede elétrica. Esta vulnerabilidade deve ser avaliada considerando a cadeia de governança e interdependência técnica do setor, centrada no ONS.

2.3 Operador Nacional do Sistema Elétrico

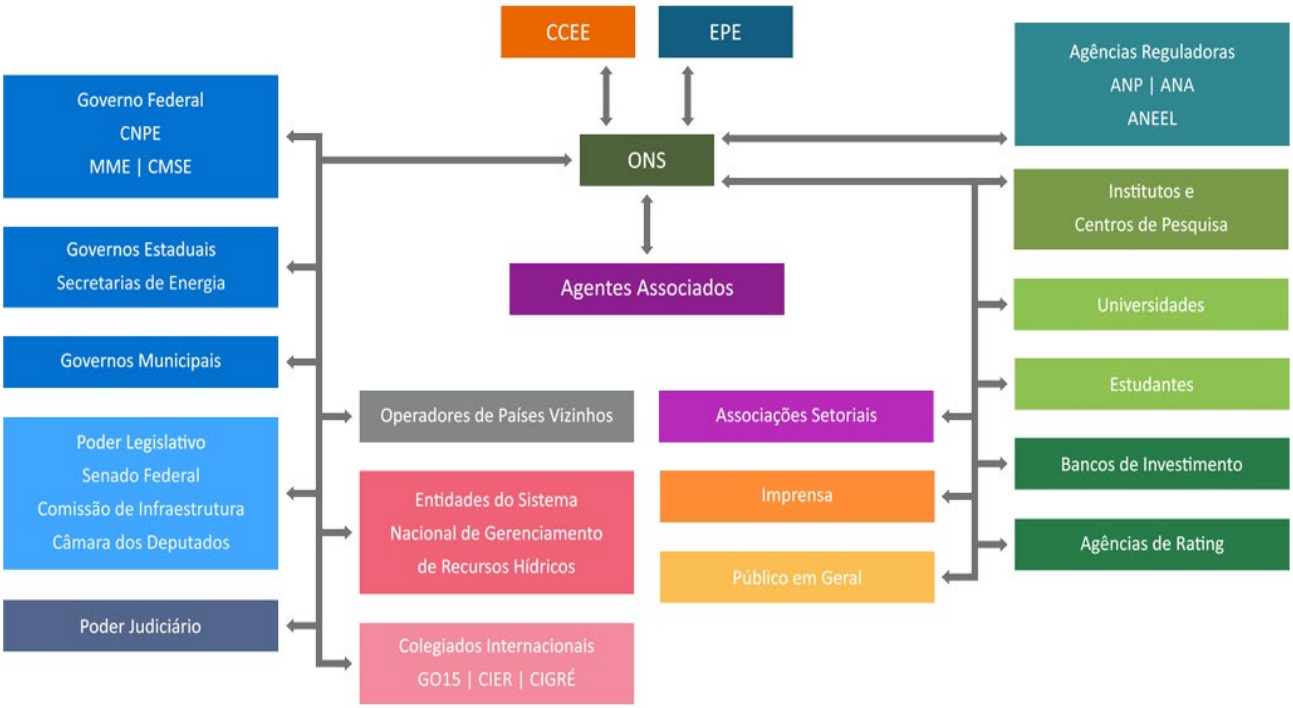
Tendo em vista o modelo do Sistema Interligado Nacional, o Brasil adota uma estrutura operacional centrada em um único Operador Independente de Sistema (ISO – *Independent System Operator*), o Operador Nacional do Sistema Elétrico. Deste modo, as atribuições do ONS são coordenar e controlar a operação das instalações de geração e de transmissão de energia elétrica no SIN, bem como planejar a operação dos sistemas isolados do país, sob a fiscalização e a regulação da Agência Nacional de Energia Elétrica (ANEEL).

Criado pela Lei nº 9.648/1998, o ONS também desenvolve uma série de estudos e ações sobre o sistema elétrico e seus agentes, de forma a garantir a segurança do suprimento contínuo de energia elétrica em todo o país. Como objetivos principais, o ONS deve (i) otimizar a operação do sistema eletroenergético, visando ao menor custo para o sistema, (ii) assegurar o acesso não discriminatório à rede de transmissão para todos os agentes do setor elétrico e (iii) contribuir para a expansão do SIN ao menor custo e nas melhores condições operacionais.

Para isto, o Operador participa de uma extensa rede de relacionamentos com diferentes organismos, agentes e instituições de diferentes segmentos da sociedade brasileira (Figura 6), incluindo o Governo Federal, os Governos Estaduais e Municipais, os órgãos legislativos federais e as agências reguladoras de água (ANA – Agência Nacional de Águas), petróleo, gás natural e biocombustíveis (ANP – Agência Nacional do Petróleo, Gás Natural e Biocombustíveis) e energia elétrica (ANEEL – Agência Nacional de Energia Elétrica).

Destaca-se que muitos destes relacionamentos decorrem das interdependências entre as já mencionadas infraestruturas críticas com o setor elétrico.

Figura 6 – Relacionamentos do ONS



Fonte: ONS, 2021.

Estruturalmente, o ONS é composto por agentes associados e membros participantes, que são as empresas de geração, transmissão e distribuição, os consumidores livres, os importadores e os exportadores de energia. Também participam do ONS o Ministério de Minas e Energia (MME) e os Conselhos de Consumidores.

2.4 Agentes do Setor Elétrico

Os agentes do setor de energia elétrica são organizados em empresas que atuam nas áreas de geração, distribuição e comercialização, e os consumidores livres e especiais, conforme o tipo de consumo e de energia.

Os geradores incluem os concessionários de serviço público, os produtores independentes e os autoprodutores.

2.5 Instalações Elétricas

As instalações elétricas que compõem o SIN são caracterizadas pela diversidade de proprietários, variando de grandes corporações a pequenos transmissores e consumidores, o que aumenta a área de exposição a ataques cibernéticos.

No setor de transmissão em particular, a evolução do mercado, com leilões de corredores de linhas de transmissão, propiciou a introdução de subestações de grande porte com múltiplos proprietários, sem uma estrutura formal de governança local, o que eleva, também, o risco de incidentes cibernéticos se propagarem de uma empresa para outra.

3. Segurança Cibernética no Brasil

A segurança cibernética no Brasil pode ser avaliada como parte da Estratégia Nacional de Transformação Digital [12], que objetiva modernizar os setores sociais e produtivos do país, através da automação e da digitalização dos processos. No setor produtivo e de serviços, isto inclui as redes de infraestruturas críticas [1][8], que suportam e catalisam a operação de todos os processos sociais, merecendo destaque e atenção especial na definição de políticas, estratégias, diretrizes, estrutura de governança e controles de segurança cibernética aplicáveis a estes setores. Estes aspectos serão avaliados como parte do macro ambiente em que se situa o Setor Elétrico Brasileiro, com foco ampliado sobre o Sistema Interligado Nacional, como parte das redes de infraestruturas críticas do país.

As subseções seguintes resumem a Estratégia Nacional de Segurança Cibernética, como parte da Estratégia de Transformação Digital, e sua implementação nas Políticas e Diretrizes de Segurança aplicáveis ao SEB. Avalia-se a implementação destas diretrizes na Estrutura de Governança e nos Sistemas de Controle das políticas de segurança cibernética nas infraestruturas críticas, com foco no setor elétrico.

3.1 Estratégia Nacional de Transformação Digital

A segurança cibernética no Brasil é considerada um dos pilares da Estratégia Brasileira para a Transformação Digital (E-Digital), instituída pelo Decreto nº 9.319/2018 [12], que criou o Sistema Nacional para a Transformação Digital (SinDigital) e foi regulamentado pelo Ministério da Ciência, Tecnologia e Inovações. Concebida para modernizar a administração pública brasileira, a E-Digital propõe-se a harmonizar as ações ligadas ao ambiente digital, aproveitando o potencial das tecnologias digitais para promover o aumento de competitividade, de produtividade e dos níveis de emprego e renda no país, de modo a alavancar o desenvolvimento econômico e social sustentável e inclusivo, com inovação.

Dois conjuntos de eixos temáticos foram estabelecidos para organizar as iniciativas de transformação: os eixos habilitadores e os eixos de transformação digital. Os eixos habilitadores objetivam o desenvolvimento da infraestrutura e o acesso às tecnologias de informação e comunicação, com ênfase na pesquisa, no desenvolvimento, na inovação, na confiança no ambiente digital, na educação e na capacitação profissional e na dimensão internacional. Já os eixos de transformação digital buscam o desenvolvimento da transformação digital da economia, com foco na cidadania e na transformação digital do Governo.

Em função da complexidade e da dimensão do espaço de segurança cibernética, nos eixos habilitadores da E-Digital, constam explicitamente [12] a necessidade da criação de mecanismos de cooperação a nível nacional para:

- "*Aprimorar os mecanismos de proteção de direitos no meio digital, inclusive nos aspectos relativos à privacidade e à proteção de dados pessoais, e reconhecer as especificidades desse ambiente;*" e
- "*Fortalecer a segurança cibernética no país, com estabelecimento de mecanismos de cooperação entre entes governamentais, entes federados e setor privado, com vistas à adoção de melhores práticas, coordenação de resposta a incidentes e proteção da infraestrutura crítica*."

Em decorrência da Política Nacional de Segurança da Informação e considerando a segurança cibernética como a área mais crítica e atual a ser abordada, o Gabinete de Segurança Institucional (GSI) deflagou as ações, a partir de janeiro de 2019, para definir a Estratégia Nacional de Segurança Cibernética (E-Ciber) [15] como primeiro módulo da Estratégia Nacional de Segurança da Informação.

Entre as ações tomadas naquele ano, consta o convite à Organização dos Estados Americanos (OEA) para realizar uma avaliação crítica da segurança cibernética no Brasil, utilizando o Modelo de Maturidade da Capacidade de Segurança Cibernética (CMM – *Capability Maturity Model*) [20] do *Global Cyber Security Capacity Centre* (GCSCC) da OEA, que define as cinco dimensões da capacidade de segurança cibernética, a seguir apresentadas:

- Política e Estratégia de Segurança Cibernética;
- Cultura Cibernética e Sociedade;
- Educação em Segurança Cibernética, Treinamento e Habilidades;
- Marcos Legais e Regulatórios; e
- Normas, Organizações e Tecnologias.

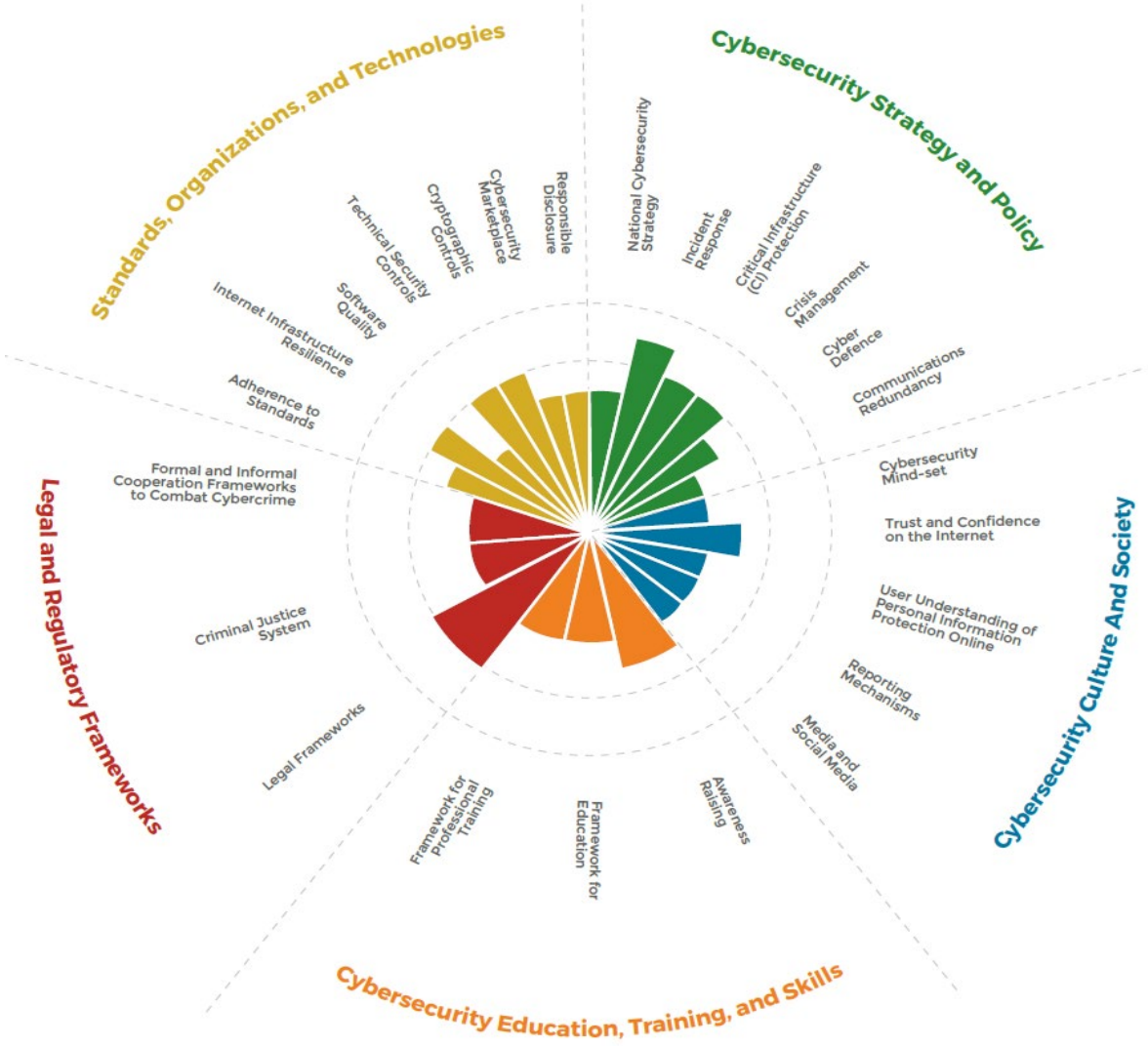
Cada dimensão é composta por uma série de fatores que avalia a capacidade de segurança cibernética. Cada um destes fatores é composto de vários aspectos, para os quais existem indicadores que descrevem etapas e ações que, uma vez observadas, definem o estado de maturidade nacional desse aspecto.

A metodologia adota cinco estágios de maturidade, desde a fase inicial até a fase dinâmica. O estágio inicial implica uma abordagem *ad hoc* ou estática da capacidade de adaptação, enquanto o estágio dinâmico representa uma abordagem estratégica com capacidade de adaptação dinâmica ou de mudança em resposta às considerações ambientais.

Participaram das entrevistas realizadas pela OEA diversos representantes da Academia, dos operadores nacionais de infraestruturas críticas, dos provedores de telecomunicações, dos ministérios governamentais, do Poder Judiciário, dos órgãos de segurança, da comunidade de defesa, do setor financeiro, das equipes de resposta a emergências computacional (CERT - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança), da mídia, do setor privado e da sociedade civil, produzindo uma avaliação, representada na Figura 7, para todos os fatores adotados na metodologia CMM.

Observa-se que cada dimensão ocupa um quinto do gráfico, com os valores de cada fator representados a partir do seu centro. O nível *"start-up"* é o mais próximo do centro do gráfico, enquanto que o nível "dinâmico" é colocado no perímetro.

Figura 7 – Capacidade de Segurança Cibernética no Brasil



Fonte: GCSCC e OAS, 2019.

3.2 Estratégia Nacional de Segurança Cibernética

Como parte da estratégia de segurança de um país, o espaço cibernético é visto como vital em qualquer plano de defesa, considerando que a soberania nacional pode ser ameaçada no plano físico, exigindo ações das forças armadas, ou no plano virtual, demandando ações de segurança do espaço cibernético [9]. Qualquer estratégia adotada deve consolidar os conceitos e identificar os principais desafios para a atividade de segurança das infraestruturas críticas, com a definição dos eixos estruturantes e dos objetivos estratégicos da digitalização da sociedade.

Como objetivos principais, constam a prevenção de possíveis interrupções das atividades relacionados às infraestruturas críticas ou a redução dos impactos dela resultantes. Para isto, é indispensável a identificação das infraestruturas críticas do país e de suas relações de interdependência, seguida da integração de dados sobre incidentes, ameaças e tecnologias de segurança e de gestão de riscos aplicáveis e da promoção de medidas de conscientização do papel destas infraestruturas na preservação da defesa e da segurança nacional.

A E-Ciber foi construída com participação de diversos setores da sociedade, formados por mais de quarenta órgãos e entidades da Administração Pública, além de instituições privadas e do setor acadêmico. Este movimento incluiu um diagnóstico da segurança cibernética internacional e nacional, que serviu para estabelecer os objetivos estratégicos nacionais e suas respectivas ações, segundo sete eixos de atuação.

De particular interesse para a segurança cibernética do setor elétrico, a recomendação para elevação do nível de proteção do Governo [15] consiste em "*elaborar requisitos específicos de segurança cibernética relativos ao uso de* endpoints *nas organizações públicas, aqui entendidos, em suma, como equipamentos finais conectados a um terminal de alguma rede ou a algum sistema de comunicação*."

Ademais, segundo a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC) [17], é necessário "*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."

Assim, a E-Ciber baseia-se em quatro princípios norteadores [17]:

- Análise de Riscos Continuada, para que a prevenção e a resiliência sejam considerados em investimentos atuais e futuros;
- Atuação Integrada, com parcerias entre o Governo Federal e o setor privado;
- Redução de Custos para a Sociedade, para que a prevenção e a resiliência sejam considerados em investimentos atuais e futuros; e
- Defesa e Segurança Nacional, para garantir a soberania política e defender a integridade territorial.

Especificamente para os setores de infraestruturas críticas, a E-Ciber definiu como ações necessárias para elevação do nível de proteção e resiliência [17]:

- *"Promover a interação entre as agências reguladoras de infraestruturas críticas para tratar de temas relativos à segurança cibernética;*
- *Estimular a adoção de ações de segurança cibernética pelas infraestruturas críticas;*
- *Incentivar que essas organizações implementem políticas de segurança cibernética, que contemplem, dentre outros aspectos, métricas, mecanismos de avaliação e de revisão periódica;*
- *Incentivar a constituição de CTIRs;*
- *Estimular que as infraestruturas críticas notifiquem o CTIR-Gov dos incidentes cibernéticos; e*
- *Incentivar a participação das infraestruturas críticas em exercícios cibernéticos."*

Destaca-se que a transformação digital da economia inclui, também, a automação das redes de infraestruturas críticas, responsáveis pela modernização e pelo desenvolvimento do país, o que demanda um conjunto consistente de Políticas Públicas de Segurança, apresentado a seguir.

3.3 Políticas Públicas de Segurança

No Brasil, a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), estabelecida pelo Decreto nº 9.573/2018 [10], foi instituída com os objetivos de garantir a segurança e a resiliência das infraestruturas críticas do país, bem como a continuidade da prestação de seus serviços. A PNSIC caracterizou a segurança de infraestruturas críticas como "*uma atividade de Estado, sinalizando à sociedade brasileira a prioridade que o Governo brasileiro atribui ao tema no âmbito da segurança institucional*." Além disso, o Decreto nº 9.573/2018 definiu as competências para o acompanhamento dos assuntos pertinentes às infraestruturas críticas no âmbito da administração pública federal.

Por segurança de infraestruturas críticas, ainda segundo o Decreto nº 9.573/2018 [10], entende-se o conjunto de medidas, de caráter preventivo e reativo, destinadas a preservar ou restabelecer a prestação dos serviços relacionados às infraestruturas críticas. Entre outras medidas, estabeleceu-se a obrigatoriedade de a Administração Pública Federal estabelecer ações de planejamento que concorram para a segurança das infraestruturas críticas. Contudo, aos demais agentes nos setores de infraestruturas críticas, que não sejam dependentes de recursos do Tesouro Nacional, a PNSIC orienta a inclusão, em seus planejamentos, de ações que concorram para a segurança das infraestruturas críticas [10].

Nota-se que não são poucos os desafios para a implementação da PNSIC, dentre os quais o Decreto nº 9.573/2018 destaca [17]:

- O reconhecimento da PNSIC como política de Estado;
- O comprometimento da Administração Pública e do setor privado;
- A consolidação da cultura de segurança;
- A elaboração de políticas públicas que fomentem a conscientização, a capacitação e a educação;
- A institucionalização da gestão de riscos;
- A criação de normas que contemplem uma estrutura de governança;
- A ampliação do treinamento e da capacitação das partes interessadas;

- A responsabilização no cumprimento dos objetivos estabelecidos para a segurança de infraestruturas críticas;
- A superação dos entraves institucionais de forma articulada;
- A integração das estruturas de comando e controle dos setores público e privado;
- A obtenção da sinergia entre os diversos setores;
- A priorização orçamentária para a execução de ações relacionadas à prevenção e à reação;
- A estruturação e o compartilhamento dos dados qualificados;
- A implementação de tecnologias e dispositivos voltados à segurança;
- O estabelecimento de canais de comunicação entre a Administração Pública e as entidades privadas; e
- A criação de um ambiente que proporcione confiança e colaboração.

O enfrentamento destes desafios, porém, envolve iniciativas estratégicas em quatro eixos estruturantes, descritas no Decreto nº 9.573/2018 [17]:

- A articulação institucional;
- A conscientização e a capacitação;
- O fomento às ações; e
- A gestão de dados e informações.

Além da prevenção de ataques e do monitoramento de incidentes, cabe à PNSIC estabelecer diretrizes para a manutenção da resiliência ou para a capacidade de as infraestruturas críticas se recuperarem após a ocorrência de ataques às suas redes. Entre as diretrizes estabelecidas, constam a prevenção e a precaução de incidentes, através da análise de riscos e da integração das diferentes esferas do poder público, do setor empresarial e dos demais segmentos da sociedade, assim como a salvaguarda do interesse da defesa e da segurança nacional.

Concomitante com a PNSIC, a Política Nacional de Segurança da Informação (PNSI), constituída pelo Decreto nº 9.673/2018 [11], estabelece diretrizes para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a

nível nacional, como forma de garantir a segurança cibernética, a defesa cibernética, a segurança física e a proteção de dados pessoais e organizacionais.

Como princípios gerais, a PNSI guia-se, principalmente, pela preservação da soberania nacional, pelo respeito aos direitos humanos e pelas garantias fundamentais de liberdade de expressão, proteção de dados pessoais, privacidade e acesso à informação. Para isto, a PNSI promove uma visão sistêmica e responsável da segurança da informação, baseada no intercâmbio científico e tecnológico entre os órgãos e as entidades da Administração Pública Federal e na educação como alicerce fundamental ao fomento de sua cultura.

A gestão de riscos e da segurança da informação é recomendada como forma de prevenção e tratamento de incidentes, através da articulação entre a segurança e defesa cibernética com a proteção de dados e ativos da informação. Assim, a PNSI prevê, também, o dever de os órgãos, as entidades e os agentes públicos garantirem o sigilo das informações imprescindíveis à segurança da sociedade e do Estado, bem como a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas [11].

Como critérios gerais de proteção, a PNSI estabelece o princípio da necessidade em conhecer (*need to know*) para acessar a informação sigilosa, garantida pela legislação, o consentimento do proprietário da informação sigilosa recebida de outros países, assim como a cooperação entre os órgãos de investigação e os órgãos públicos no processo de credenciamento de pessoas que terão acesso às informações sigilosas. A Política estabelece, ainda, a necessidade de integração e cooperação entre o poder público, o setor empresarial, a sociedade e as instituições acadêmicas e a cooperação internacional, no campo da segurança da informação.

3.4 Diretrizes de Segurança Cibernética

As estratégias e as políticas nacionais de segurança cibernética, para serem efetivas, devem ser traduzidas em diretrizes concretas, que norteiem as ações necessárias tanto para os setores vitais e de infraestruturas críticas, quanto para os cidadãos e processos sociais.

No Brasil, as diretrizes de segurança cibernética são derivadas das diretrizes nacionais do E-Digital, através de um engajamento permanente com a comunidade científica, o setor produtivo e a sociedade civil. As diretrizes nacionais de segurança cibernética incluem, ainda, o fortalecimento da articulação e da cooperação entre os diferentes órgãos e entidades do poder público com competências relacionadas à temática digital. Entre as principais diretrizes, consta o incentivo ao compartilhamento de informações e à análise do impacto de iniciativas setoriais no ambiente digital, visando à harmonização e à promoção de eficiência e sinergia entre as ações de diferentes órgãos e entidades [12].

Nos setores críticos das infraestruturas nacionais, para a implementação da política nacional de segurança cibernética, a PNSIC estabelece diretrizes básicas de integração, cooperação e incentivo às ações que garantam a preservação da integridade das infraestruturas críticas do país [10]. Isto inclui uma estreita integração e cooperação entre órgãos e entidades federais, estaduais, distritais e municipais, através de seus sistemas de gerenciamento e monitoramento de incidentes. Esta integração deve ocorrer pela cooperação e por parcerias entre os setores público e privado nacionais e entidades internacionais afins, sob a direção do Sistema Brasileiro de Inteligência.

A permuta de informações e o intercâmbio de conhecimentos são considerados vitais para o sucesso destas diretivas, no tempo e no volume corretos, como prerrequisito à identificação e à execução das ações necessárias, em sintonia com a evolução doutrinária e tecnológica da segurança cibernética. Pela dimensão, complexidade e interdependência das infraestruturas críticas do país, um sistema de governança, a nível nacional, se faz necessário para gerir a política de segurança e acompanhar sua implementação em todos os setores vitais.

Especificamente para a segurança da informação, a PNSI estabelece diretrizes para garantir a segurança do indivíduo, da sociedade e do Estado, através da segurança da informação utilizada na Administração Pública e no setor privado, de modo a preservar os direitos e as garantias fundamentais [11]. Neste sentido, deve-se fomentar a pesquisa científica, o desenvolvimento tecnológico e as inovações relacionadas à segurança da informação, mediante a formação e a qualificação dos recursos humanos, traduzidas em melhorias contínuas no arcabouço legal e normativo, na cultura da segurança da informação e na preservação da memória cultural brasileira.

Mais especificamente, a PNSI estabelece ações relacionadas à custódia de dados por entidades públicas e à proteção das informações das pessoas físicas que possam ter sua segurança ou a segurança das suas atividades afetada, garantindo as restrições de acesso necessárias e implementando uma estrutura adequada de governança, a nível público e dentro das organizações.

3.5 Governança da Segurança Cibernética

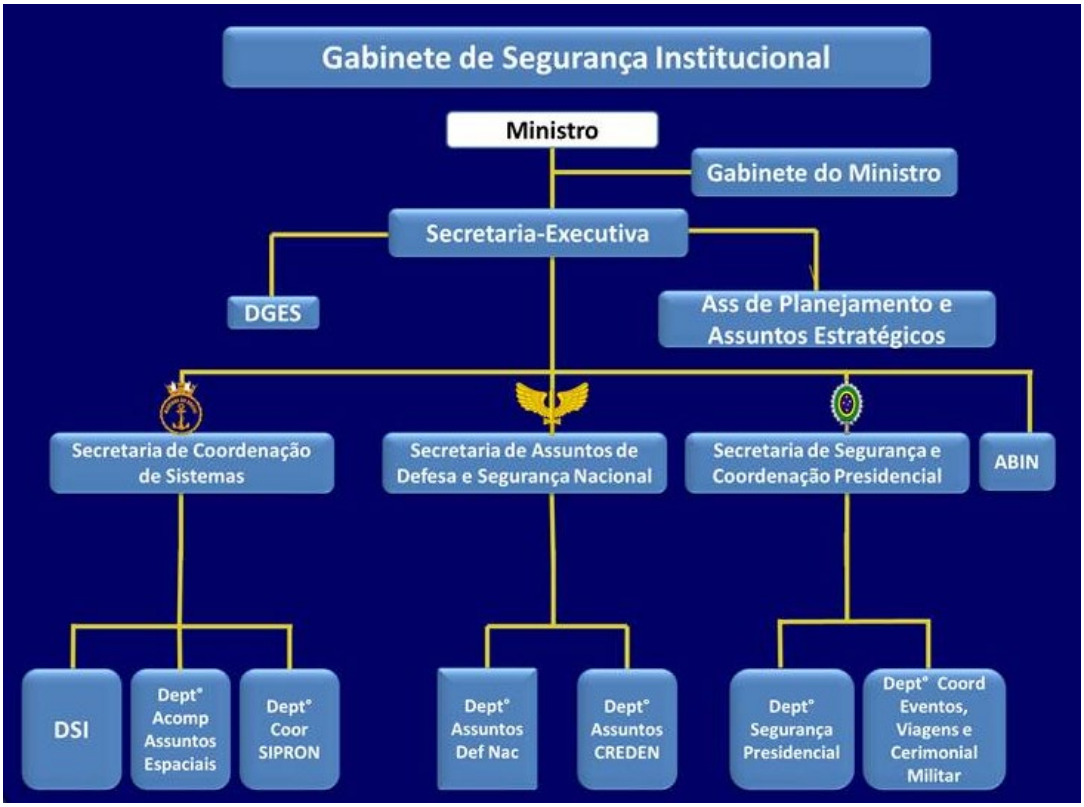
A governança da segurança cibernética objetiva alinhar o planejamento com as ações estratégicas, a otimização do uso de recursos, a melhoria da qualidade dos serviços prestados e a condução exitosa de projetos e de processos. Na segurança cibernética, considerando a profusão de atores relacionados, o planejamento adquire especial relevância, amplificada pela capilaridade e pela transversalidade do tema em diferentes áreas da sociedade, e interdependência entre os diversos setores sociotécnicos e de infraestrutura.

No Brasil, a estrutura de governança da segurança cibernética é distribuída pela Administração Pública Federal, sob o comando de órgãos ligados diretamente à Presidência da República. Esta estrutura é suportada por vários instrumentos regulatórios, definidos por meio de decretos presidenciais.

O nível mais alto de governança da segurança cibernética no país concentra-se na Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, à qual compete analisar, discutir e propor ao Presidente da República a ENSIC e o PNSIC [10].

A implementação das políticas de segurança cibernética no Brasil, assim como o SinDigital, encontra-se sob a responsabilidade do Gabinete de Segurança Institucional da Presidência da República (Figura 8) e do Centro de Defesa Cibernética do Exército Brasileiro, vinculado ao Ministério da Defesa (CDCiber/EB/MD). O Comitê Interministerial para a Transformação Digital (CITDigital), composto por representantes do poder público federal, o Conselho Consultivo para a Transformação Digital, composto por especialistas e representantes da comunidade científica de notório saber, da sociedade civil e do setor produtivo, e demais órgãos, entidades e instâncias vinculados às políticas de transformação digital também são coordenados pelo GSI.

Figura 8 – Organização do Gabinete de Segurança Institucional



Fonte: GOV.BR, 2021.

Ao GSI compete, principalmente, as funções de planejar, coordenar e metodizar as atividades de segurança cibernética e da informação e comunicações na Administração Pública Federal, bem como de operacionalizar e manter um Centro de Tratamento e Resposta a Incidentes (CSIRT, de *Computer Security Incident Response Team*) ocorridos nas redes de computadores da Administração Pública Federal. No Brasil, existem oito tipos de Centros de Tratamento e Resposta aos Incidentes Cibernéticos [15], classificados de acordo com sua atuação, conforme apresentado abaixo:

- Centros de Responsabilidade Nacional;
- Centros de Coordenação Internacional;
- Centros de Infraestruturas Críticas;
- Centros de Provedores;
- Centros Corporativos;
- Centros Acadêmicos;
- Centros do Poder Público; e
- Centros Militares.

Entre outras atribuições, estes centros possuem mecanismos para monitorar vulnerabilidades das entidades associadas, adulterações e indisponibilidade de sítios, anúncios de vazamento de informações e redes sociais abertas. Adicionalmente, estes centros agem em cooperação com órgãos parceiros em segurança cibernética, ao integrar uma rede internacional de CSIRTs, com a realização de intercâmbios para analisar possíveis ações massivas de ataques.

Ao GSI compete, ainda, o apoio na elaboração dos planos nacionais temáticos e na definição de critérios e normas para monitorar e avaliar a execução da PNSI e de seus instrumentos, bem como auxilia no estabelecimento dos requisitos mínimos de segurança para produtos utilizados na administração que incorporem recursos de segurança da informação [11].

Na esfera militar, o Centro de Defesa Cibernética do Exército Brasileiro (CDCiber) define a Política Cibernética de Defesa, visando orientar, no âmbito do Ministério da Defesa, as atividades de Defesa Cibernética, no nível estratégico, e de Guerra

Cibernética, nos níveis operacional e tático. Ao Ministério da Defesa compete, especificamente, elaborar as diretrizes, os dispositivos e os procedimentos de defesa que atuem nos sistemas relacionados à defesa nacional contra ataques cibernéticos [11].

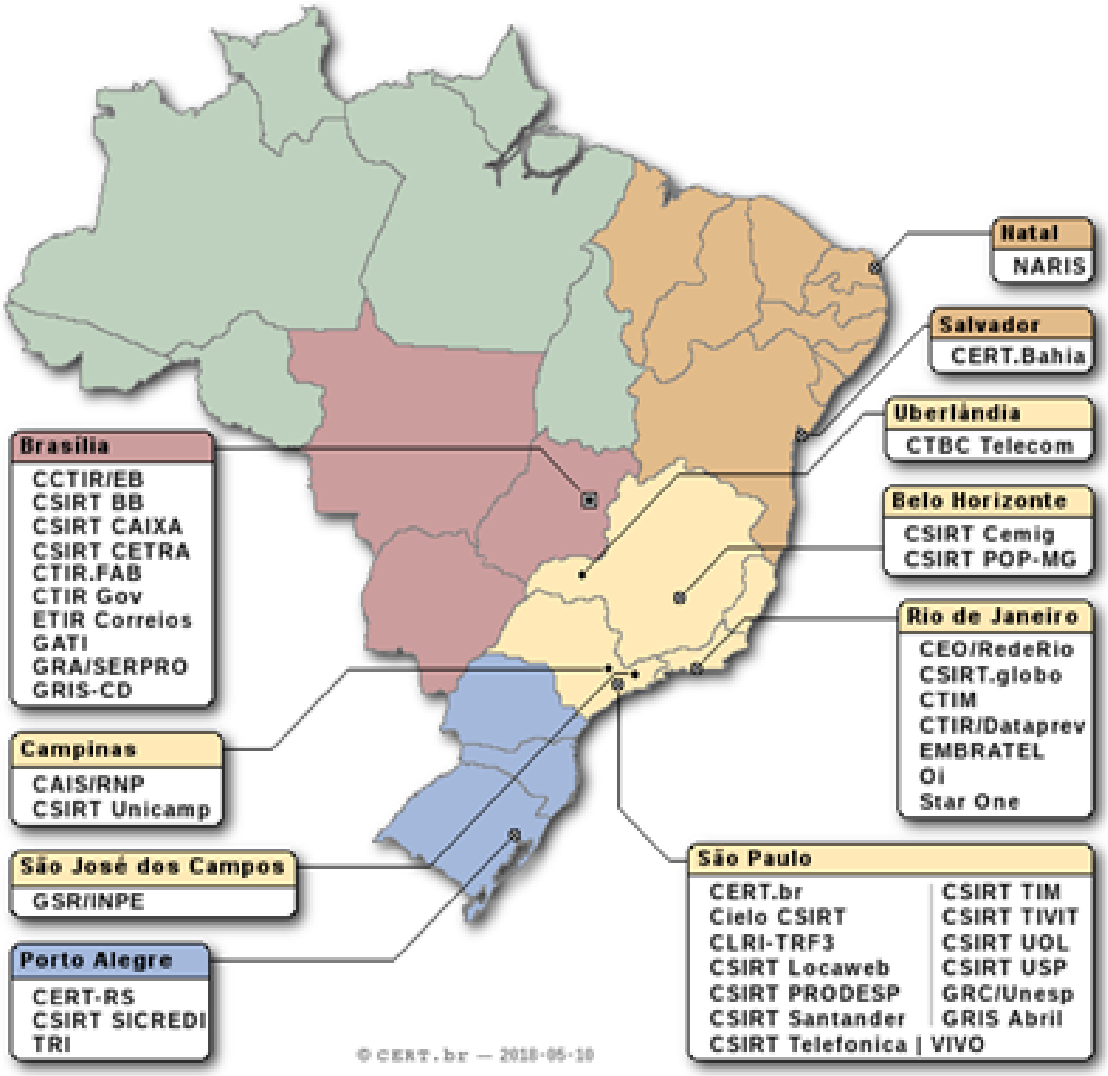
Além destas unidades estratégicas, duas outras entidades exercem o papel de controlar e monitorar os indicadores relacionados a incidentes de segurança, sendo elas o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores (CTIR) e o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT) [7].

O CTIR está subordinado ao Departamento de Segurança de Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, com a função principal de atender aos incidentes em redes de computadores da Administração Pública Federal, mediante a notificação, a análise e a coordenação de resposta de incidentes, o que inclui a distribuição de alertas, recomendações e estatísticas.

O CERT é mantido pelo Núcleo de Informação e Coordenação (NIC.br), do Comitê Gestor da Internet no Brasil, acessível a qualquer rede brasileira conectada à internet. Entre seus objetivos, destacam-se a análise de estatísticas e tendências de ataques e suas melhores formas de combate e proteção, unificando as informações de incidentes de segurança oriundas de diversas entidades.

A Figura 9 ilustra a distribuição dos CERTs no território nacional, na qual se observa que apenas o CSIRT Cemig se localiza em uma empresa de energia elétrica e a completa ausência destes organismos na Região Norte.

Figura 9 – Número de CERTs no Brasil



Fonte: CERT, 2019.

Especificamente para a segurança da informação, a PNSI instituiu o Comitê Gestor da Segurança da Informação, com função de assessorar o GSI nas atividades relacionadas ao tema [11]. Este comitê é composto por membros do GSI e da Casa Civil, com a participação da maioria dos órgãos da Administração Pública Federal, entre os quais os Ministérios da Justiça e Segurança Pública, da Defesa, das Relações Exteriores, da Economia, da Infraestrutura, da Agricultura, Pecuária e Abastecimento, da Educação,

da Cidadania, da Saúde, de Minas e Energia, da Ciência, Tecnologia e Inovações, do Meio Ambiente, do Turismo, do Desenvolvimento Regional e da Mulher, da Família e dos Direitos Humanos, a Controladoria-Geral da União, a Secretaria Geral da Presidência da República, a Secretaria de Governo da Presidência da República, a Advocacia-Geral da União e o Banco Central do Brasil.

Para garantir a segurança da informação, o GSI, assessorado pelo Comitê Gestor da Segurança da Informação, normatiza os requisitos metodológicos para a implementação da gestão de risco dos ativos da informação pelos órgãos da Administração Pública Federal, traduzidos em programas sobre segurança da informação, bem como na conscientização e na capacitação dos servidores públicos federais e da sociedade. Adicionalmente, o Comitê Gestor da Segurança da Informação acompanha a evolução doutrinária e tecnológica, em âmbito nacional e internacional, do tema da segurança da informação, definindo a Estratégia Nacional de Segurança da Informação e a PNSI, em sintonia com o Comitê Interministerial para a Transformação Digital, criado pelo Decreto nº 9.319/2018 [12].

Às demais entidades subordinadas da Administração Pública Federal compete a implementação dos planos temáticos da PNSI, em especial no que diz respeito a sua definição e as suas normas internas. A alta administração destas entidades define a governança da segurança da informação interna, observando a simplificação administrativa, a modernização e a integração da gestão pública, o monitoramento do desempenho da segurança da informação e a execução de programas, de projetos e de processos relativos à temática, segundo diretrizes de gestão de riscos.

Além disso, na definição da governança, deve-se estabelecer um sistema de gestão de segurança da informação que garanta a comunicação imediata, ao Centro de Tratamento de Incidentes de Redes do GSI, da existência de vulnerabilidades ou incidentes que impactem ou possam impactar os serviços prestados ou contratados pelos respectivos órgãos subordinados a cada entidade da Administração Pública Federal. Neste sentido, cada órgão da Administração Pública Federal possui um Gestor de Segurança da Informação interno e um Comitê de Segurança da Informação, ou estrutura equivalente, para deliberar sobre os assuntos relativos à PNSI.

No que diz respeito ao orçamento, verba pública é alocada para possibilitar ações de segurança da informação e para promover a capacitação e a profissionalização dos recursos humanos em temas relacionados. Ademais, uma equipe de treinamento e resposta a incidentes em redes computacionais é instituída em cada órgão da Administração Pública Federal, coordenada pelo Centro de Tratamento de Incidentes de Redes do GSI. Esta equipe, espelhada na estrutura organizacional de cada entidade, coordena e executa as ações de segurança da informação no âmbito de sua atuação, auditando a gestão de segurança e aplicando as ações corretivas e disciplinares cabíveis nos casos de violação de normas [11]. Em particular, a equipe assessora a implementação das ações de segurança da informação e a proposição de políticas e normas internas sobre a temática.

De especial importância para a segurança da informação, constam os requisitos para a garantia da interoperabilidade de tecnologias, processos, informações e dados, através da interação dos ativos de informação do Governo Federal ou daqueles sob sua custódia, evitando a fragmentação das bases de informação de interesse público e da sociedade, bem como integrando, padronizando e compartilhando as redes de telecomunicações da Administração Pública Federal.

Além das normas de governança propostas pelo GSI, a Estratégia Nacional de Segurança Cibernética [15] sugere a consulta e a observância, quando aplicável, das normas correlatas da Organização Internacional para Padronização (ISO, do inglês *International Standards Organization*), do *Control Objectives for Information and Related Technology* (COBIT23), do *National Institute of Standards and Technology* (NIST24) e do *Center for Internet Security* (CIS25), de modo a garantir a adoção de controles customizados e medidas de segurança, específicos para cada modelo de negócio.

3.6 Controles das Políticas de Segurança

Visando garantir os resultados de uma estratégica de segurança, mecanismos devem ser criados para acompanhar e assegurar o cumprimento das diretrizes demandadas em cada nível da Administração Pública. Para isso, a ENSIC é suportada por dois instrumentos de controle estratégicos: a PNSIC e o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas [10].

A PNSIC reúne as orientações gerais para a implementação da segurança das infraestruturas críticas do país, difundindo os fundamentos necessários à elaboração de planos setoriais e à atribuição de responsabilidades aos órgãos executores. Para isto, recomenda-se a definição das áreas prioritárias para aplicação dos planos setoriais, com o envolvimento dos órgãos federais, estaduais, municipais e da sociedade, de modo a se estabelecer as responsabilidades e periodicidade das ações e implementar a gestão de riscos e a análise de interdependência.

O segundo instrumento de controle da PNSIC refere-se ao Sistema Integrado de Dados de Segurança de Infraestruturas Críticas, gerido pelo GSI e destinado ao registro informatizado dos ativos e das condições de segurança das infraestruturas críticas nacionais, incluindo a coleta, o tratamento, o armazenamento e a recuperação de informações, bem como a avaliação de riscos cibernéticos. O Sistema Integrado de Dados de Segurança de Infraestruturas Críticas deve ser utilizado, principalmente, no apoio às decisões e como uma base de informações para a elaboração de relatórios de segurança de infraestruturas críticas.

Simultaneamente, para a proteção da informação, a PNSI estabelece como principais instrumentos de gestão a Estratégia Nacional de Segurança da Informação e os planos nacionais organizados por temas relacionados [11].

A Estratégia Nacional de Segurança da Informação define as ações estratégicas e os objetivos relacionados à segurança da informação, incluindo a segurança e defesa cibernética da informação, em particular contra o vazamento de dados que possam comprometer a segurança das infraestruturas críticas. Destaque-se o requisito da ampla participação da sociedade e do poder público em sua construção.

Os planos nacionais temáticos, por sua vez, são alocados a órgãos de controle específicos, destinados ao detalhamento das ações estratégicas e dos objetivos da Estratégia Nacional de Segurança da Informação, incluindo o planejamento, a organização e a coordenação das atividades e do uso de recursos e a definição de responsabilidades, cronogramas, análises de riscos e gestão de ações de contingência [11].

4. Segurança Cibernética de Setores Críticos

A exemplo dos demais setores críticos da sociedade, a exposição do Setor Elétrico Brasileiro a ataques cibernéticos decorre da sua própria modernização, mediante a introdução da automação e da digitalização das instalações elétricas, da operação remota com telecomunicações e dos controles e sistemas operacionais adotados. Além da capilaridade com as demais redes sociotécnicas, o setor elétrico depende diretamente de três campos tecnológicos que amplificam a superfície de ataques cibernéticos, que se complementam e se superpõem na gestão do Sistema Interligado Nacional (Figura 10): a Tecnologia Informática, a Tecnologia Operacional e a Tecnologia de Telecomunicações.

Figura 10 – Domínios Tecnológicos

Fonte: SIQUEIRA, 2018.

A Tecnologia Operacional compreende os sistemas e processos computacionais utilizados para proteger, comandar e monitorar a operação dos ativos elétricos. A Tecnologia Informática, por outro lado, abrange os sistemas e processos informacionais utilizados para gerenciar e administrar a organização.

Já a Tecnologia de Telecomunicações envolve os sistemas, processos e meios de comunicação utilizados para interligar os ativos elétricos, operacionais e informáticos, dentro e fora da corporação. Para todos estes campos, que se complementam na operação do SIN, é necessária a definição de uma estratégia de proteção contra ataques cibernéticos.

Para a proteção de uma infraestrutura crítica como o setor elétrico, com elevados níveis de interação entre as áreas de Operação, Telecomunicações e Informática e interligado com outros setores sociotécnicos, sugere-se a adoção de uma estratégia progressiva como parte de uma agenda regulatória nacional, seguindo uma abordagem de cima para baixo (*topdown*).

Esta abordagem deve incluir as etapas de definição de estratégia, análise de risco, definição de políticas, definição de controles e, finalmente, monitoramento e auditoria das soluções tecnológicas específicas do setor adotadas pelos agentes, conforme representado na Figura 11. Para todas estas camadas, sugerem-se abordagens genéricas e agnósticas quanto a fornecedores e soluções comerciais, facilitando sua adoção pelos agentes do mercado de energia. Por fim, o trabalho de regulamentação, controle e auditoria deve ser realizado pela ANEEL.

Figura 11 – Estratégia para uma Agenda Regulatória

Fonte: SIQUEIRA, 2018.

A seguir, propõe-se um arcabouço teórico para a definição de estratégias de proteção cibernética para setores de infraestrutura críticas, adequada a redes sociotécnicas de extensão nacional, que podem ser desdobradas em políticas de segurança e em controles de implementação viáveis de regulamentação, de auditoria e verificação de conformidade por órgãos reguladores. O arcabouço proposto é exemplificado com as características da arquitetura cibernética do SEB, relacionadas com sua hierarquia funcional e de governança, suas tecnologias e vulnerabilidades a ataques cibernéticos.

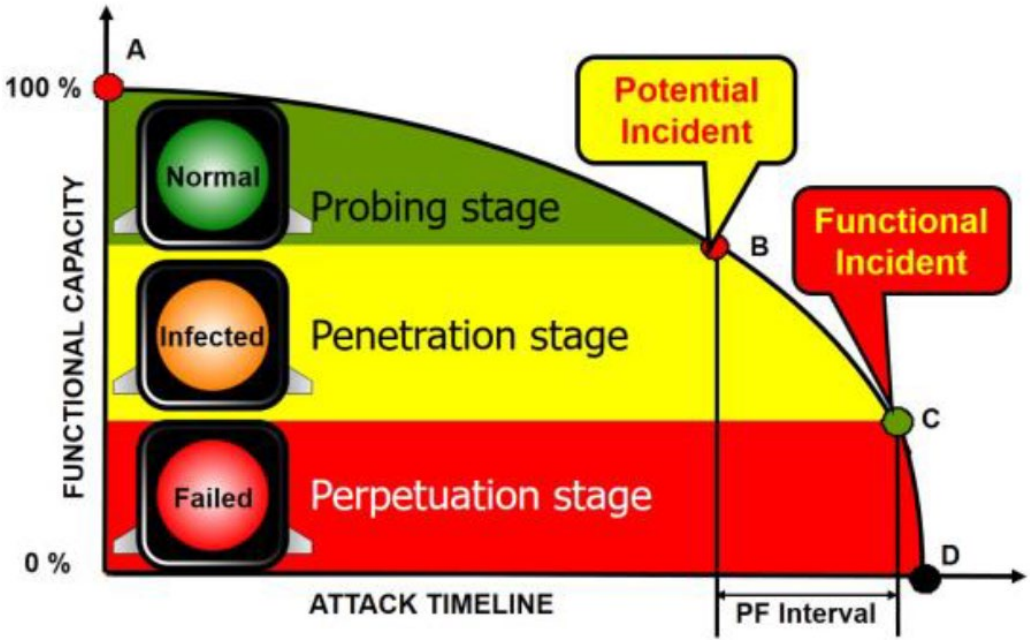
Destaca-se que a abordagem é suportada por um conjunto abstrato de estratégias, políticas e contramedidas, ilustradas por conjuntos de ícones gráficos que facilitam sua documentação e inclusão em uma discussão nacional sobre a regulamentação do tema. O capítulo se encerra com uma proposta de abordagem regulatória, para discussão pelos diferentes setores e agentes, de governança e de auditoria, aplicável aos diferentes domínios de segurança recomendados para cada nível hierárquico do SEB.

4.1 Estratégias de Segurança Cibernética

Uma estratégia de segurança objetiva definir, a um nível elevado de abstração, as classes de políticas de proteção cibernética recomendadas para cada estágio de evolução de ataques comuns a um determinado setor sociotécnico. Para definição destas estratégias, é útil classificar os níveis de gravidade de incidentes de forma abstrata, considerando a penetração de possíveis ataques cibernéticos nas redes sociotécnicas.

Estes níveis podem ser identificados através de um gráfico temporal de evolução típica de um ataque a uma infraestrutura crítica, dividido em três estágios, conforme ilustrado na Figura 12.

Figura 12 – Estágios de um Ataque Cibernético



Fonte: SIQUEIRA, 2018.

Estes estágios, identificados por faixas coloridas na Figura 12, diferenciam a capacidade funcional da infraestrutura crítica ao longo de seu ciclo de operação, conforme o nível de penetração de um ataque e delimitadas pelas condições indicadas no semáforo da Figura 12, de acordo com as definições a seguir.

- Normal: capaz de atender à sua finalidade ou, durante a tentativa de um ataque cibernético, antes de uma penetração ou possível incidente;
- Infectado: com a degradação da capacidade funcional, durante o estágio de penetração do ataque cibernético, antes da perpetuação em um incidente; ou
- Falho: incapaz de cumprir com sua finalidade ou, durante a perpetuação de um ataque cibernético, após uma falha funcional.

Estes estágios são temporalmente delimitados por dois tipos de incidentes:

- Incidente Potencial: condição mensurável e identificável que sinaliza uma degradação funcional pendente ou em processo de ocorrência, após um estágio de tentativa (*probing stage*) de um ataque cibernético que explora uma vulnerabilidade de uma infraestrutura crítica; ou

- Incidente Funcional: incapacidade de um sistema executar uma função específica entre os limites de desempenho desejados, após o estágio de penetração (*penetration stage*) de um ataque cibernético a uma infraestrutura crítica, iniciando o estágio de perpetuação (*perpetuation stage*).

Uma estratégia de segurança consiste na definição da política recomendada para a proteção da infraestrutura em cada estágio de contaminação, tendo em vista as seguranças intrínsecas dos sistemas protegidos e as características observáveis dos incidentes provocados pelos ataques, mensuradas através dos incidentes potenciais e funcionais da infraestrutura, podendo ser classificadas, genericamente, em três classes abstratas de estratégias:

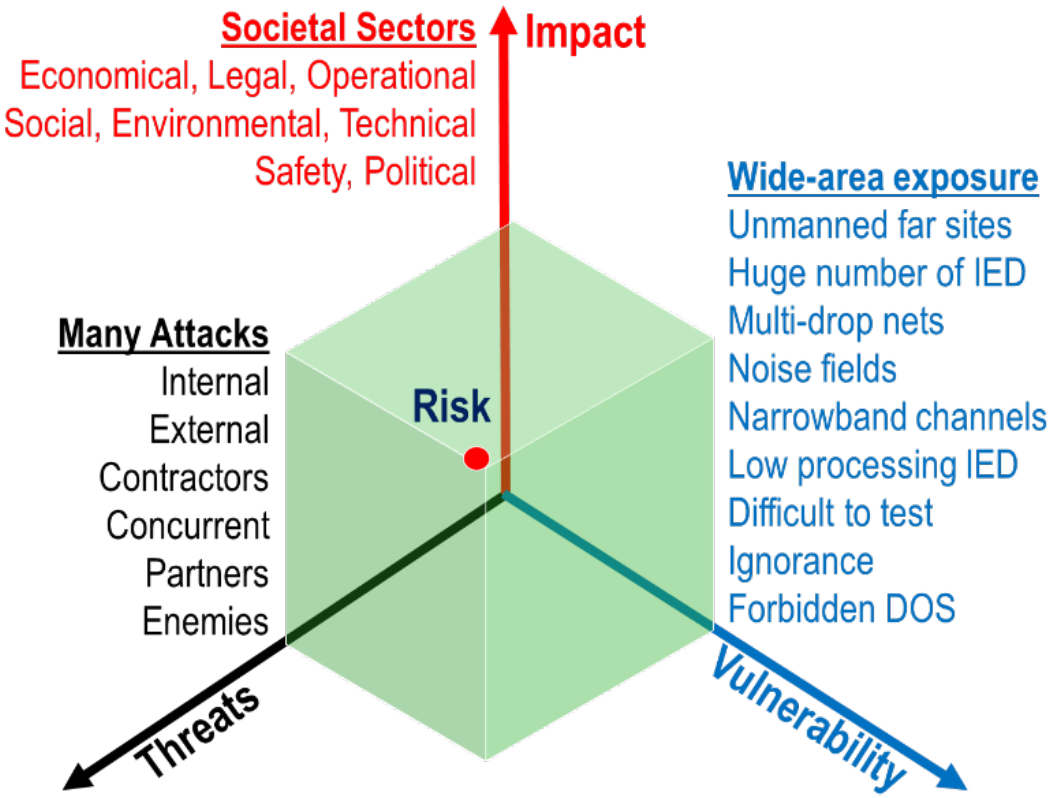
- Prevenção: políticas aplicáveis na prevenção de ataques cibernéticos;
- Correção: políticas aplicáveis na correção da funcionalidade após um ataque cibernético, mas antes da interrupção total da funcionalidade da infraestrutura; ou
- Recuperação: políticas aplicáveis na recuperação da capacidade funcional de uma infraestrutura, após a perpetuação de um ataque cibernético.

Destaca-se que a escolha das políticas aplicáveis a cada estágio de penetração de ataques deve ser suportada por uma análise de risco das consequências da perpetuação do ataque.

4.2 Análise de Risco Cibernético

O risco de um ataque cibernético às infraestruturas do SEB deve ser avaliado considerando o contexto específico deste setor e seu papel catalizador entre as demais infraestruturas críticas nacionais. A Figura 13 traduz o contexto desta análise de risco em um espaço tridimensional, cujos eixos consideram as vulnerabilidades próprias do SIN, sua exposição a ataques e os impactos possíveis destes incidentes.

Figura 13 – Análise de Riscos Cibernéticos



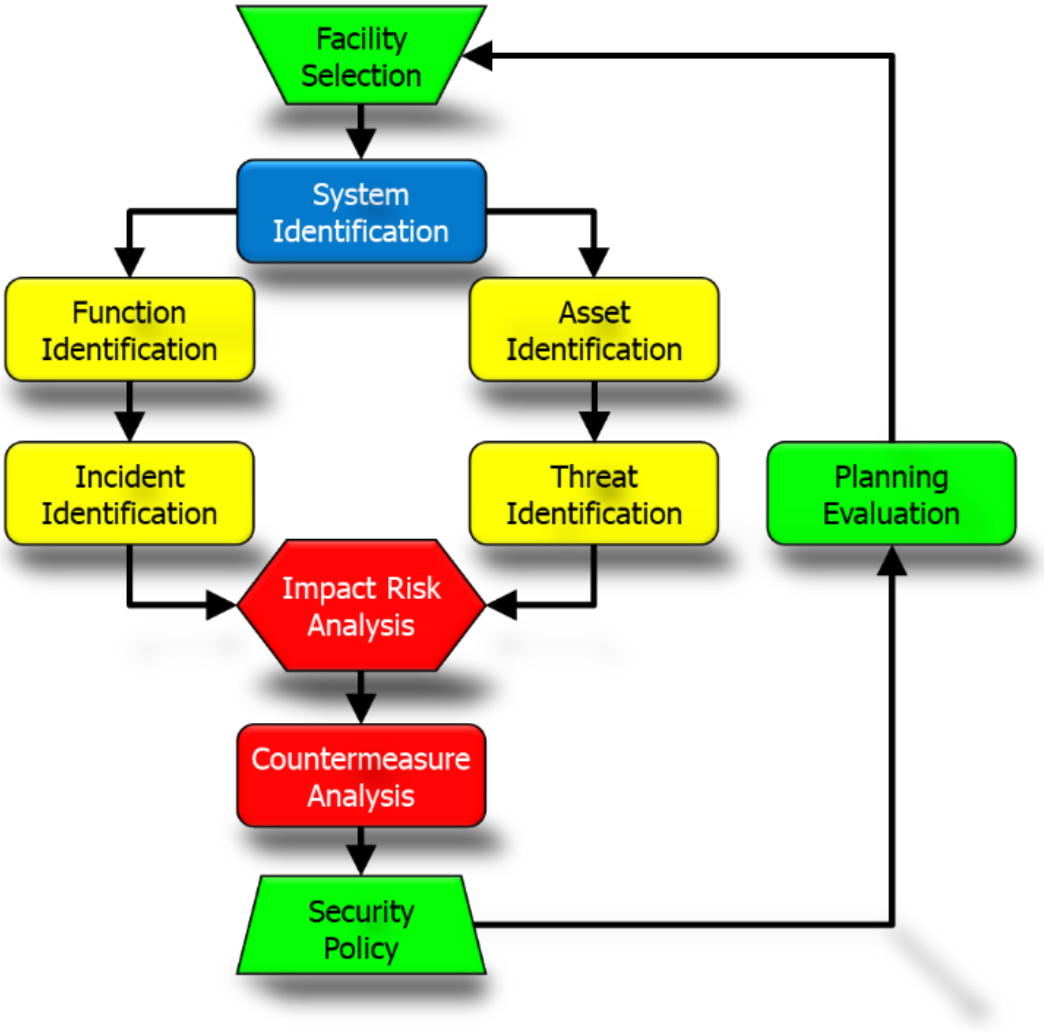
Fonte: SIQUEIRA, 2018.

Diversos *frameworks* existem para analisar estes riscos cibernéticos de forma a dar suporte à definição de políticas de segurança, entre aqueles normatizados internacionalmente por ISO [31], IEC [32] [33] e ISA [42] ou por sociedades profissionais internacionais, como o CIGRE [34] [35] [36] [37] [38] e o IEEE [40], organismos nacionais americanos, como o NERC [41], NIST [39] e o USDOE/USDHS [43], ou brasileiros, como a ABNT [44][45], . O tema também é profusamente documentado em diversos livros textos relacionados à análise de riscos em infraestruturas críticas [46] [47] [48] [49] [50].

Neste sentido, a Figura 14 ilustra um possível fluxograma para avaliar o risco e a seleção de políticas, comum à maioria destes *frameworks*, que inclui a escolha das instalações, a identificação dos sistemas funcionais destas instalações,

de seus ativos e funções ativas, bem como de ameaças e incidentes, a análise dos riscos dos impactos da perpetuação dos ataques e a análise das contramedidas possíveis, visando a formação da política de proteção adequada.

Figura 14 – Planejamento de Segurança Cibernética



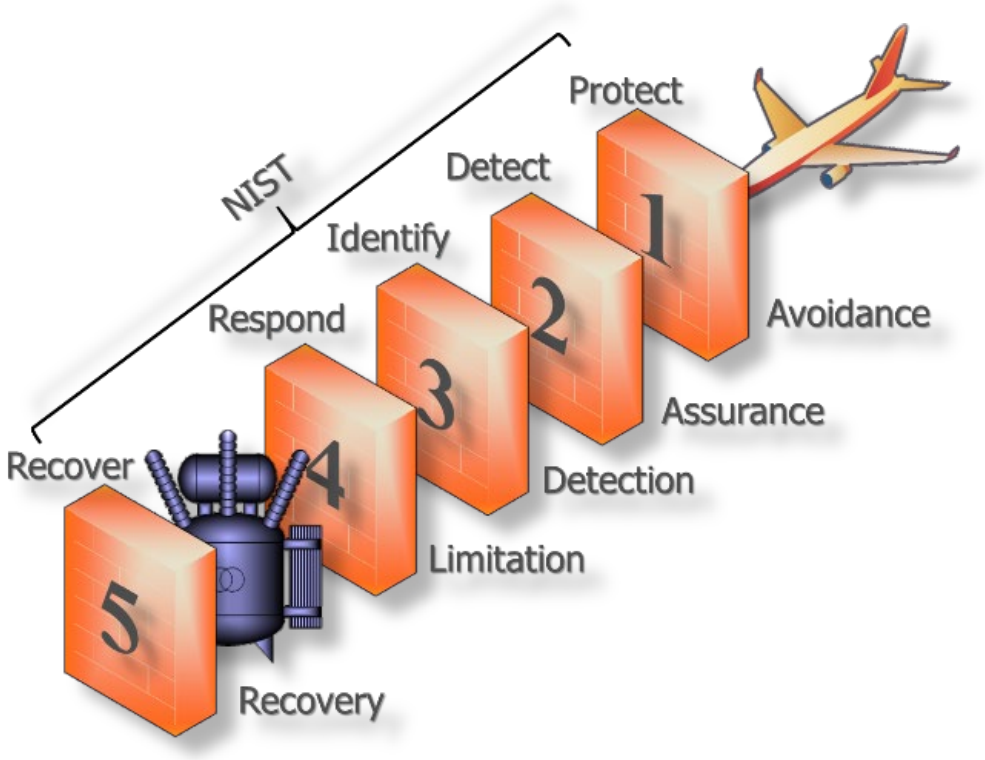
Fonte: SIQUEIRA, 2018.

Nota-se que o problema regulatório consiste, essencialmente, em escolher ou adaptar um destes *frameworks* e avaliar suas recomendações à luz das características e necessidades nacionais. Alguns países adotaram as normas NIST americanas como ponto de referência e as subseções seguintes sugerem algumas classes de políticas propostas como partida para uma regulamentação nacional do tema.

4.3 Políticas de Segurança Cibernética

Uma estratégia racional de segurança para o SEB pode ser derivada de um conjunto mínimo de classes abstratas de políticas de segurança, recomendadas em função da importância de cada sistema, de sua vulnerabilidade a ataques e pelas consequências de sua perpetuação nas infraestruturas críticas afetadas [2]. O principal princípio de uma política de segurança refere-se à implementação de barreiras sucessivas ou de proteção em profundidade, para tentar barrar o nível de penetração de um ataque através de obstáculos sucessivos [2] [3] [4] [5]. A Figura 15 ilustra este conceito, tomando como base as camadas de proteção sugeridas pelas normas NIST [39] americanas.

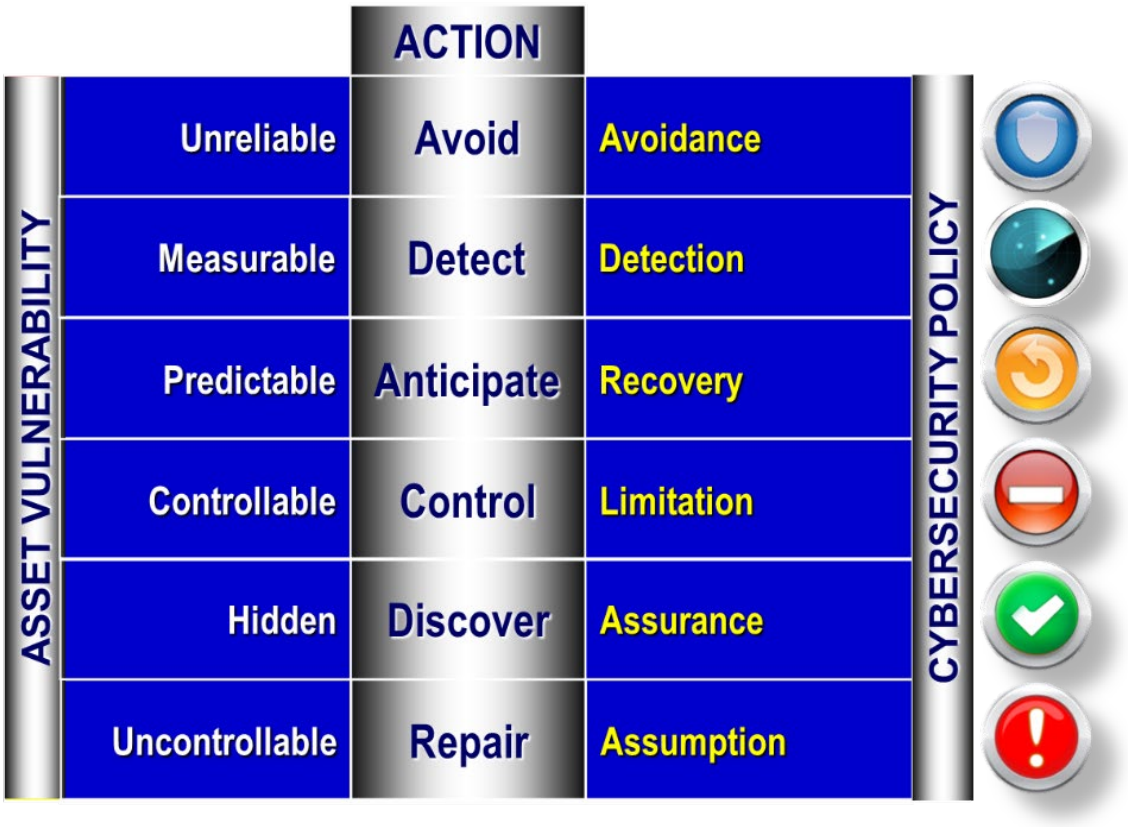
Figura 15 – Defesa Cibernética em Profundidade



Fonte: SIQUEIRA, 2018.

A Figura 16, a seguir, ilustra uma possível estratégia de proteção, sugerida com base nos *frameworks*, aplicável a qualquer infraestrutura crítica, correlacionado a melhor política de prevenção com o tipo de vulnerabilidade da infraestrutura e a observabilidade dos incidentes de segurança.

Figura 16 – Políticas de Segurança Cibernética



Fonte: SIQUEIRA, 2018.

A tabela da Figura 16 permite a utilização de um processo de decisão estruturado, com a finalidade de selecionar as políticas de proteção adequadas para combater as consequências dos ataques, em função das vulnerabilidades das infraestruturas críticas do SEB.

As políticas são selecionadas a partir de um conjunto de políticas padronizadas, listadas na terceira coluna da tabela da Figura 16, correlacionadas com as classes de vulnerabilidades próprias da infraestrutura e classificadas de acordo com a seguinte lista:

- Não confiável (*Unreliable*): impossível suportar ou aceitar as consequências dos ataques;
- Mensurável (*Measurable*): possível avaliar o nível de penetração do ataque por inspeção;

- Previsível (*Predictable*): possível estimar, com dados passados, o instante para o próximo ataque;
- Controlável (*Controllable*): possível alterar a taxa de ocorrência dos ataques;
- Oculto (*Hidden*): impossível saber da contaminação sem um teste funcional; ou
- Incontrolável (*Uncontrollable*): impossível de evitar, mas suportado pela resiliência da infraestrutura.

Com base nesta classificação, a Tabela 2 sugere a política de segurança mais adequada, entre as políticas padronizadas listadas na Figura 16, associadas a uma simbologia gráfica para utilização na arquitetura de segurança.

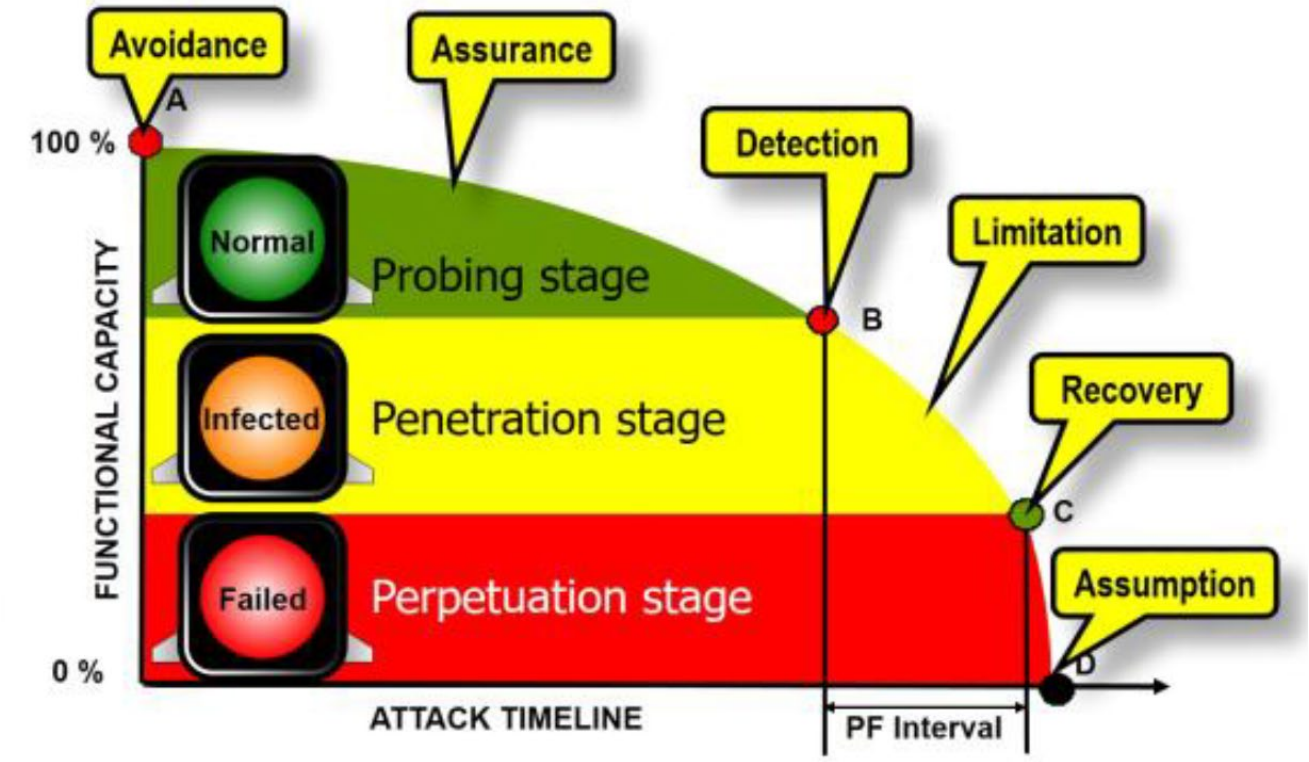
Tabela 2 – Políticas de Segurança Cibernética

Símbolo	Política	Significado
	Evasão (*Avoidance*)	Modificar o *design* de ativos cibernéticos para reduzir os incidentes cibernéticos
	Detecção (*Detection*)	Detectar possíveis incidentes cibernéticos por meio de inspeção ou medição adequada antes da perpetuação
	Recuperação (*Recovery*)	Recuperar de um ataque antes de um incidente cibernético através de contramedidas de rotina
	Limitação (*Limitation*)	Aplicar contramedidas ao usuário, além das pessoas de TI ou TO
	Garantia (*Assurance*)	Descobrir incidentes ocultos por meio de testes funcionais adequados
	Assunção (*Assumption*)	Recuperar de um incidente cibernético após sua perpetuação

Fonte: Adaptado de SIQUEIRA, 2018 e AMOROSO, 2012.

Normalmente, essas políticas são aplicáveis a diferentes instantes da linha do tempo dos ataques cibernéticos, como apresentado na Figura 17.

Figura 17 – Linha temporal das Políticas de Proteção



Fonte: SIQUEIRA, 2018.

As políticas de Evasão e Garantia são aplicáveis quando a função da infraestrutura se encontra no estado Normal. As políticas de Detecção e Limitação, por outro lado, são mais adequadas durante a fase de infecção ou estado Anormal do ataque cibernético. Já as políticas de Recuperação e Assunção aplicam-se, principalmente, na fase de consumação ou estado de Falha da funcionalidade da infraestrutura.

A escolha da classe de política de proteção para cada funcionalidade e fase da linha de ataque da rede de infraestrutura será decorrente da análise de riscos, conforme descrito na subseção anterior. Dependendo desta análise, definem-se os controles de segurança cibernética aplicáveis a cada política, em cada estágio da linha de ataque da Figura 17.

4.4 Controles de Segurança Cibernética

Definidas as políticas de acordo com as funcionalidades do SEB, os controles de segurança aplicáveis a cada domínio cibernético também podem ser selecionados de um conjunto de classes padronizadas, dependendo da política escolhida.

Para cada domínio de segurança, são aplicáveis medidas e controles específicos, seguindo as recomendações da IEC padrão 62351 [25] para sistemas de automação, conforme a política selecionada.

Dependendo do contexto, as medidas e os controles específicos podem ser aplicados a um domínio inteiro de segurança (incluindo todos os seus ativos e meios de comunicação) ou a um ativo específico em um domínio, como um servidor ou protocolo de comunicação.

Neste caso, recomenda-se, também, a adoção de um conjunto de classes padronizadas, associadas a símbolos gráficos padronizados, que facilitem a especificação das soluções de segurança utilizadas em cada domínio cibernético, com base em sua arquitetura funcional.

Ademais, os controles de segurança devem, preferencialmente, ser definidos a partir de um conjunto padronizado de classes de recomendações, adaptadas da norma IEC 62351 [25] ou [28], identificadas por um grupo de símbolos gráficos padronizados, representados na Tabela 3, que podem ser sobrepostos aos diagramas das camadas da arquitetura de referência do SEB, como requisitos mínimos de controles de segurança.

Tabela 3 – Simbologia para Controles de Segurança

Símbolo	Controle	Significado
	Enganação (*Deception*)	Funcionalidade/informação enganosa
	Ocultação (*Discretion*)	Ocultação de informações confidenciais
	Separação (*Separation*)	Imposição de restrições de acesso
	Coleção (*Collection*)	Coleta automatizada de informações
	Diversidade (*Diversity*)	Uso intencional de diferentes tecnologias
	Correlação (*Correlation*)	Análise de informações coletadas
	Semelhança (*Commonality*)	Adoção de melhores práticas de segurança
	Consciência (*Awareness*)	Compreensão do *status* anormal
	Profundidade (*Depth*)	Imposição de múltiplas camadas de segurança
	Resposta (*Response*)	Reação planejada ao estado Anormal

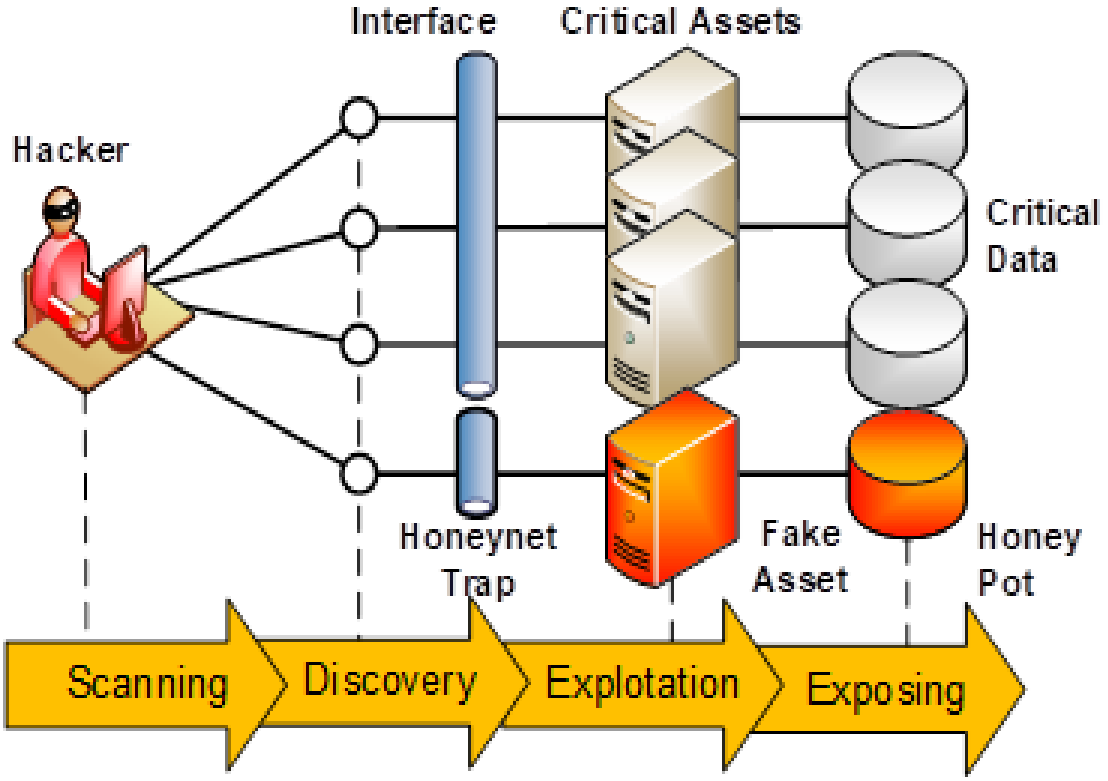
Fonte: Adaptado de SIQUEIRA, 2018 e AMOROSO, 2012.

A seguir, são resumidas as principais características destas dez classes de contramedidas, com exemplos de implementação.

Uma contramedida de Enganação é a introdução de uma funcionalidade ou informação enganosa (*fake*) para induzir o *hacker* ao erro.

Por exemplo, conforme apresentado na Figura 18, citam-se uma funcionalidade enganosa (*honeypot* ou *honeynet*) atraente e local, externamente acessível a *hackers* maliciosos internos e externos, e um sistema de gerenciamento de *honeypot* ou *honeynet* para detectar tentativas de exploração e disparo de respostas de proteção.

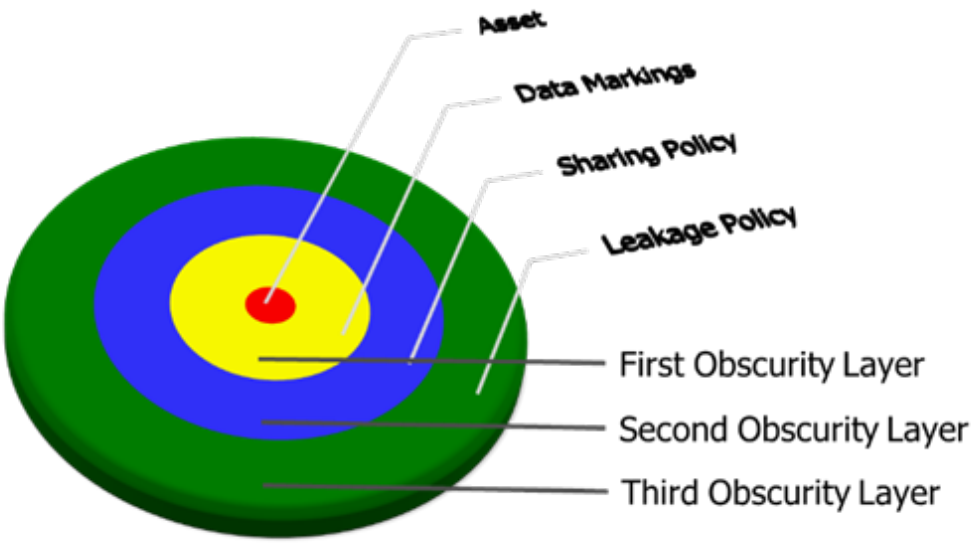
Figura 18 – Contramedida de Enganação



Fonte: SIQUEIRA, 2018.

Uma contramedida de Ocultação consiste em tornar secretas ou obscuras determinadas informações ou funcionalidades, mantendo-as desconhecidas para os *hackers* e seguindo uma hierarquia de obscuridade. Como exemplo, conforme consta Figura 19, têm-se as informações organizacionais devidamente marcadas e tais marcas adequadamente aplicadas e uma equipe organizacional totalmente treinada sobre as políticas locais de tratamento das informações e compartilhamento externo.

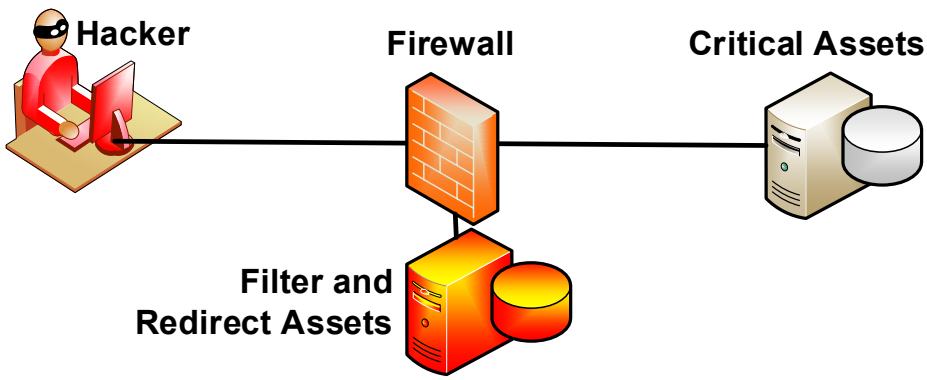
Figura 19 – Contramedida de Ocultação



Fonte: SIQUEIRA, 2018.

Uma contramedida de Separação representa a imposição de barreiras ou restrições de acesso, limitando a ativos e pessoas autorizadas. A Figura 20 apresenta dois exemplos, quais sejam, o redirecionamento ou a filtragem do tráfego de ataque em tempo real antes de atingir os pontos de entrada da rede local e a imposição de controles de acesso à rede (*firewalls*, DMZ ou VPN) entre grupos de ativos internos, recursos organizacionais e qualquer rede externa não confiável.

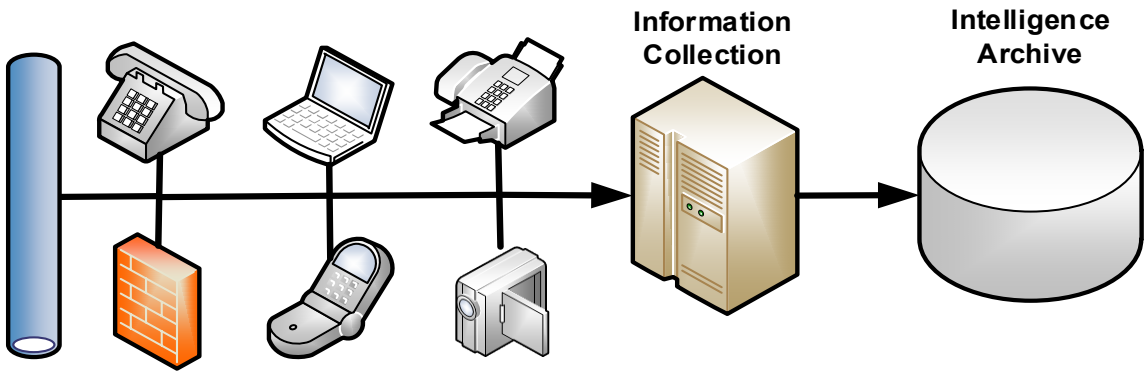
Figura 20 – Contramedida de Separação



Fonte: SIQUEIRA, 2018.

Uma contramedida de Coleção é a coleta automatizada de informações em tempo real sobre processos e sistemas, principalmente referente aos acessos a ativos protegidos. Na Figura 21, constam dois exemplos, os critérios para o estabelecimento de quais tipos de informações e em quais contextos serão coletados e armazenados os dados e os sistemas de coleta para recolher informações em tempo real e armazená-las de forma segura, a partir de aplicativos, sistemas e redes acessadas.

Figura 21 – Contramedida de Coleção



Fonte: SIQUEIRA, 2018.

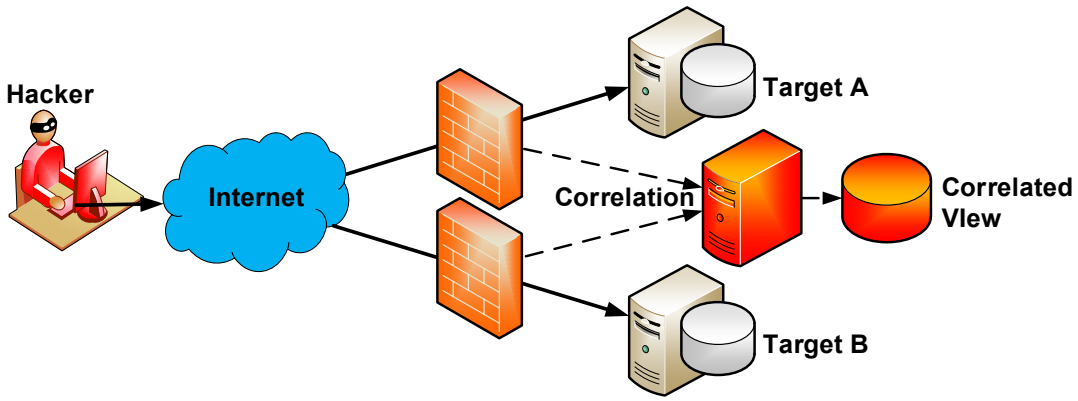
Uma contramedida de Diversidade compreende o uso proposital de tecnologias diferentes, para realização da mesma função, de modo a evitar erros comuns. Na Figura 22, é apresentado o exemplo do uso de distintos fornecedores, para que nenhum incidente de um fornecedor único possa produzir um efeito em cascata em uma funcionalidade crítica de aplicação, computação ou rede e se tenha, pelo menos, um fornecedor de *backup* ativo e alternativo para ativos de missão crítica de um fornecedor diferente.

Figura 22 – Contramedida de Diversidade

Fonte: SIQUEIRA, 2018.

Uma contramedida de Correlação consiste na análise sistemática das informações coletadas pela contramedida de Coleção. Por exemplo, algoritmos são utilizados para correlacionar informações relevantes em tempo real, de modo a deduzir resultados acionáveis, que precisem de alguma ação corretiva ou preventiva, e uma saída correlativa pode estar relacionada a uma função de conscientização e resposta organizacional na detecção de um incidente, conforme exposto na Figura 23.

Figura 23 – Contramedida de Correlação

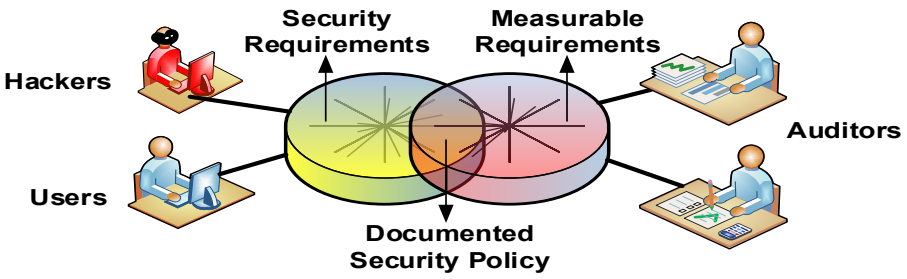


Fonte: SIQUEIRA, 2018.

Uma contramedida de Semelhança é a adoção das melhores práticas regulatórias e de mercado referentes à segurança cibernética.

Os exemplos apresentados na Figura 24 são a aplicação de políticas de segurança escritas, com treinamento de apoio para tomadores de decisão, e de mecanismos para execução e consequências de violação e a conformidade da organização com um padrão de segurança da informação reconhecido e atestado por um auditor externo.

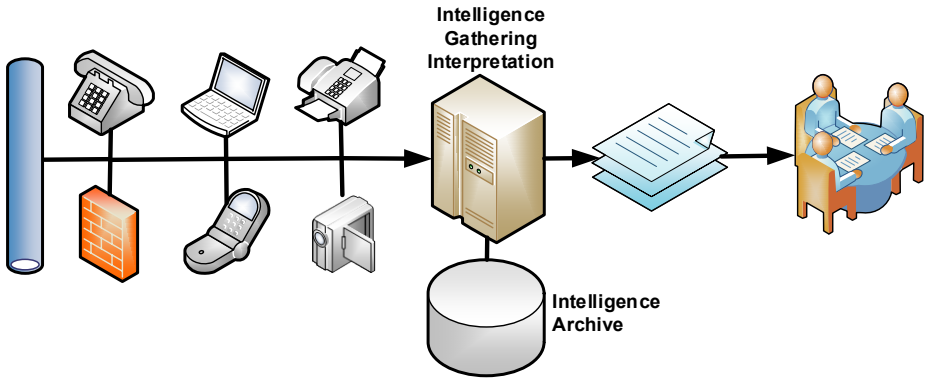
Figura 24 – Contramedida de Semelhança



Fonte: SIQUEIRA, 2018.

Uma contramedida de Consciência envolve ações orientadas para prover a organização da capacidade de compreensão do *status* de normalidade ou anormalidade, em consequência de ataques cibernéticos. Na Figura 25, constam os exemplos de coleta regular de informações de inteligência de segurança cibernética e disseminação aos tomadores de decisão em tempo hábil e operações de segurança em tempo real para garantir e coordenar quaisquer ações preventivas ou de resposta a incidentes.

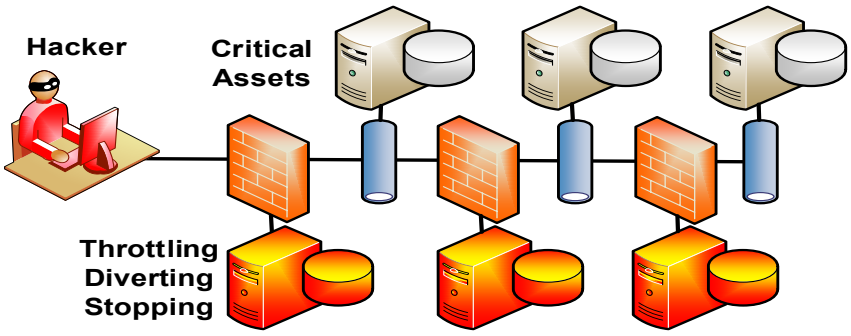
Figura 25 – Contramedida de Consciência



Fonte: SIQUEIRA, 2018.

Uma contramedida de Profundidade inclui a adoção de múltiplas camadas de segurança. A Figura 26 apresenta os exemplos de proibir qualquer acesso direto a qualquer ativo essencial sem pelo menos dois desafios de autenticação, estrangular, desviar ou parar o tráfego de ataque antes de atingir um ativo crítico e falha de um sistema de proteção não poder comprometer qualquer ativo crítico (critério N-1).

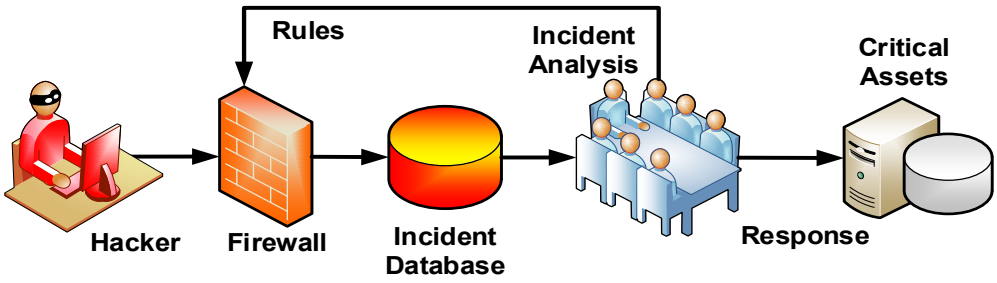
Figura 26 – Contramedida de Profundidade



Fonte: SIQUEIRA, 2018.

Por fim, uma contramedida de Resposta é a definição prévia de reações planejadas a qualquer estado Anormal, após a análise de incidentes. Por exemplo, citam-se a reação a indicadores e sinais de alerta antes de um ataque a qualquer ativo crítico e a documentação e as métricas referentes à causa raiz de problemas de segurança passados e à eficácia de atividades de resposta para incidentes de segurança, expostos na Figura 27, abaixo.

Figura 27 – Contramedida de Resposta



Fonte: SIQUEIRA, 2018.

Considerando esta lista, as contramedidas de segurança cibernética adequadas podem ser mapeadas para cada política selecionada, como é mostrado na Tabela 4, que possui o exemplo de um plano de segurança cibernética aderente a esta filosofia.

Outros planos podem ser montados, seguindo a mesma abordagem, de acordo com a análise de riscos realizada.

Tabela 4 – Plano de Segurança Cibernética

Control	Policy					
	Avoidance	Assurance	Detection	Limitation	Recovery	Assumption
Deception	misleading functionality / information	scan available ports and resources	check honey pot deception traps	periodic updating of honey pots	clean honeypot traps and data base	no misleading functionality / information
Discretion	obscuring sensitive information	try disclosing sensitive information	check the disclosure of sensitive data	periodic updating of passwords	replace broken passwords / sensitive data	allow disclosing public information
Separation	enforced access policy restrictions	try unauthorized access	check unauthorized access tentative	periodic review of security domains	rework broken firewall rules	unrestricted open access policy
Collection	automated gathering of information	simulate incident to gather information	check collected log information	periodic empting of logs	restore overloaded data base	no information gathering
Diversity	intentional use of different technologies	try to substitute a supplier	check diversity of suppliers	periodic renewing of suppliers	change disrupted technologies	use identical technologies
Correlation	analysis of collected information	try injecting correlated information	check correlation of logged information	periodic analysis of collected data	identify & block source of attacks	no analysis of incidents or information
Commonality	adoption of security best practices	try non-standard practices	check conformance audit records	periodic updating of security policies	reinforce broken security best rules	non-standardized practices
Awareness	understanding of abnormal status	simulate perception of abnormal status	check perception of incidents	periodic renewing of operator training	retrain after undetected incidents	no understanding of abnormal status
Depth	enforcing multiple security functional layers	try unauthorized cross of security layers	check logs for partial security layer breaking	periodic review of firewall rules	reinforce broken depth defenses	none or single security functional layer
Response	misleading functionality / information	simulate reaction to abnormal status	check response to simulated failures	periodic review of disaster / recovery plan	run disaster recovery plans	unplanned reaction to abnormal status

Fonte: SIQUEIRA, 2018.

4.5 Tecnologias de Segurança Cibernética

Analogamente, uma Arquitetura Tecnológica de Segurança pode ser definida a partir de um conjunto padronizado de classes de soluções ou tecnologias, agnósticas e independentes de fornecedores ou de soluções comerciais, identificadas por símbolos gráficos padronizados, derivados da norma IEC 62351-10 [25], conforme representado na Tabela 5.

Tabela 5 – Simbologia para Tecnologias de Segurança

Símbolo	Tecnologia	Significado
	*Firewalls*	Restrições de tráfego para comunicação proibida
	*Strong Authentications*	Autenticação multifatorial ou respostas de desafio
	*Domains*	Agrupamento administrativo de múltiplas redes privadas
	*RBAC*	Controle de acesso baseado em função
	*Security Option*	Alternativas específicas de segurança de protocolo
	*DMZ*	Zonas desmilitarizadas para separar Redes Locais (LANs) de redes não confiáveis
	*Data Cryptography*	Disfarce de informações para entidades não autorizadas
	*Traffic Segregation*	Rede Virtual Privada (VPN)
	*Monitoring*	Registro e gravação de eventos para auditoria
	*Virus Protection*	Detecção e remoção de vírus

Fonte: Adaptado de IEC, 2012.

Os ícones de controles e tecnologias de segurança podem ser alocados graficamente em cada camada da arquitetura do sistema sociotécnico, associando-os a domínios inteiros ou a itens específicos de cada camada, conforme sugerido pela norma IEC 62351-10 [25], de modo a gerar uma visão integrada da solução de segurança para cada nível e domínio da arquitetura do setor elétrico, o que facilita a sua auditoria e regulamentação. Estes conceitos serão ilustrados através de uma possível solução de arquitetura de segurança para o setor elétrico, incluída apenas como exemplo da abordagem sugerida, no capítulo seguinte.

5. Segurança Cibernética do Setor Elétrico Brasileiro

Definida uma abordagem estratégica para a segurança cibernética, sua aplicação ao SEB decorrerá da estrutura funcional do Sistema Interligado Nacional. No caso brasileiro, sobressaem, nesta análise, a existência de um único operador do sistema elétrico e a extensão geográfica da rede nacional. Destaca-se que os conceitos e critérios discutidos no capítulo anterior serão utilizados para exemplificar cenários de definição de estratégias, políticas, regulamentações, controles e tecnologias típicas aplicáveis ao SIN.

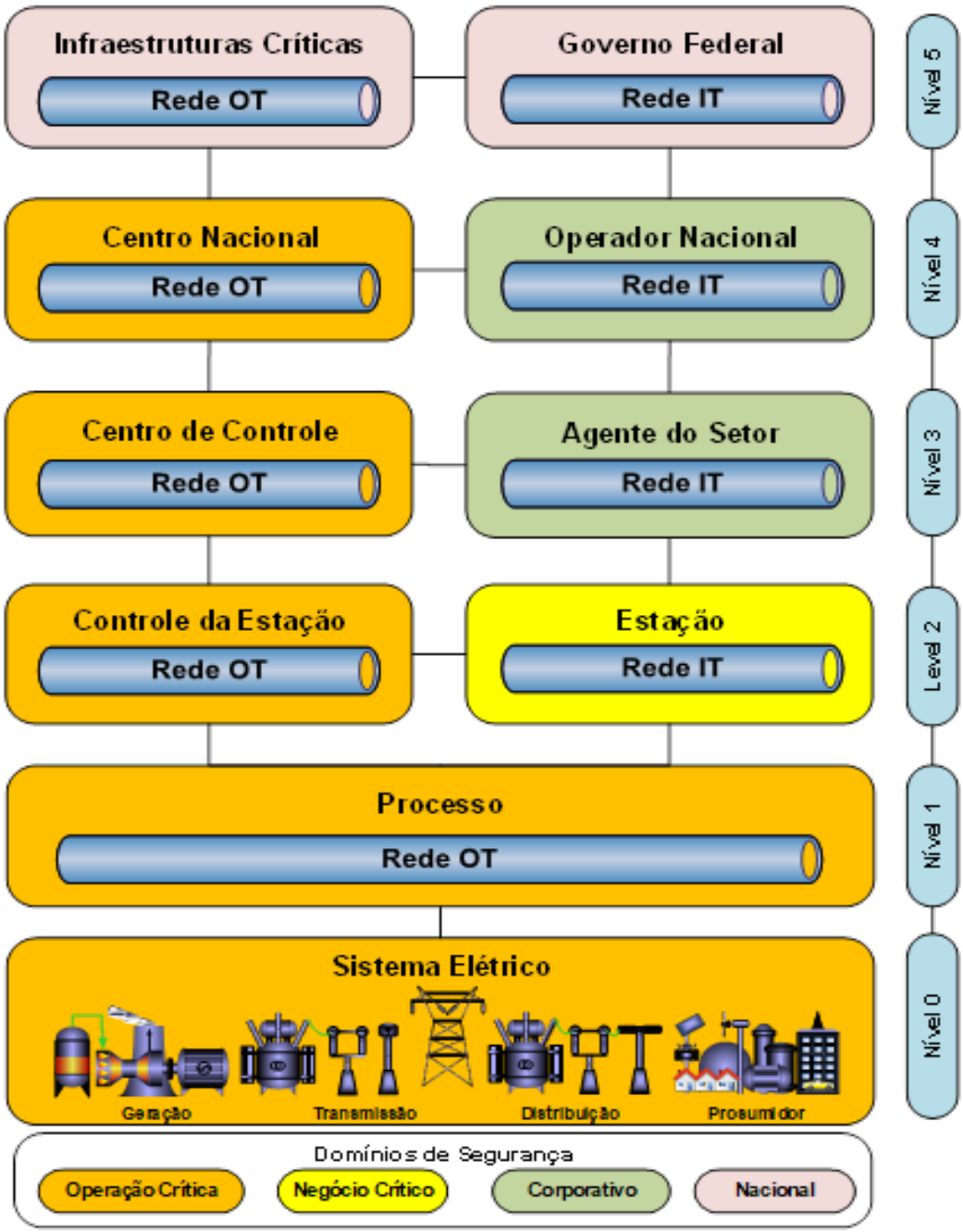
A seguir, são resumidas as sugestões para uma Estratégia Nacional de Segurança Cibernética do Setor Elétrico, com possíveis desdobramentos em políticas e controles, até a avaliação das tecnologias aplicáveis. A metodologia segue o arcabouço proposto no capítulo anterior, como sugestão de discussão com os atores interessados.

5.1 Arquitetura Cibernética

A Segurança Cibernética do Setor Elétrico pode ser avaliada considerando uma arquitetura em camadas, modelada segundo o padrão original *Purdue Enterprise Reference Architecture and Methodology* (PERA) [21] e adaptada para o contexto nacional brasileiro.

Neste sentido, a Figura 28 mostra uma visão genérica das camadas de domínios de segurança (TI/TO) a nível nacional e suas conexões (TL), derivadas deste arquétipo, que será utilizada como modelo de referência neste trabalho. Ressalta-se que este modelo é apenas conceitual, para orientar a proposição de políticas, controles e tecnologias aplicáveis de segurança cibernética ao SEB e úteis para fomentar uma discussão nacional sobre a sua regulamentação.

Figura 28 – Arquitetura Cibernética do Setor Elétrico



Fonte: Elaboração própria.

Seguindo o modelo PERA da Purdue [21], uma arquitetura de ativos de TI/TO pode ser dividida em seis camadas hierárquicas, identificadas por seis níveis numéricos, apresentados na Figura 28, que interagem ou estão relacionados por redes de comunicação (TL), conforme a classificação a seguir.

- Nível 0 – Rede de Campo;
- Nível 1 – Rede de Processos;
- Nível 2 – Rede de Estações;
- Nível 3 – Rede do Centro de Controle;
- Nível 4 – Rede Corporativa; ou
- Nível 5 – Rede Externa.

O Nível 0, equivalente à camada mais baixa, também denominado por Rede de Campo, compreende todos os itens físicos de alta e baixa tensão das instalações elétricas do SIN, ou seja, os equipamentos dos sistemas energéticos, tais como disjuntores, transformadores, reatores, geradores, etc. Genericamente, este nível refere-se a qualquer instalação física das estações de geração, transmissão, distribuição ou consumo de energia elétrica. Utilizando interfaces e protocolos de comunicação de *IoT*, todos os ativos podem se comunicar, em potencial, com outros equipamentos ou itens do mesmo nível ou camadas superiores da arquitetura.

O Nível 1, a segunda camada, também conhecido como Rede de Processos, abrange todos os ativos de *hardware* e *software* que monitoram, medem ou controlam diretamente todos os equipamentos do sistema elétrico, como barramentos, alimentadores, disjuntores, transformadores, reatores, etc. Estes ativos incluem os meios e as redes de comunicação local e os protocolos de comunicação que interligam estes equipamentos a nível de campo e se comunicam diretamente com os ativos do Nível 0.

O Nível 2, a terceira camada, também chamado de Rede de Estação, é composto por todos os itens de *hardware* e *software* que supervisionam, monitoram e controlam centralizadamente uma subestação ou usina. Estes ativos incluem, normalmente, as redes e os processadores das salas de comando, os processadores de interfaces humana, assim como os protocolos de comunicação e controle destas instalações.

O Nível 3, a quarta camada, também denominado por Rede do Centro de Controle, compreende todos os itens de *hardware* e *software* e os protocolos de comunicação que supervisionam, monitoram e controlam, a nível corporativo, as subestações e usinas

de um agente e interagem diretamente com o centro de controle do ONS. Este Nível pode possuir subníveis, dependendo da estrutura hierárquica de centros de controle utilizada por cada agente do SIN.

O Nível 4, a quinta camada, também conhecido como Rede Nacional, engloba todos os itens de *hardware* e *software* e os protocolos de TI, TL e TO do ONS que interagem com os Centros de Controle dos agentes no Nível 3, para processar tarefas operacionais, comerciais, de engenharia e administrativas, e com os demais agentes e entidades setoriais, de mercado e governamentais.

O Nível 5, a sexta camada, chamado de Rede Externa, compreende os centros de controle binacionais, internacionais e de monitoramento setorial, os centros de controle de outros setores críticos e todos os itens de entidades externas que se comunicam com o ONS na realização de atividades de negócios, operação, engenharia e administração.

Destaca-se que os níveis a partir do Nível 3 estão divididos em dois domínios relacionados aos ativos de TI e TO de todos os agentes, representando a separação típica entre estes ativos e constituindo domínios tradicionais de segurança cibernética em cada Nível.

5.2 Domínios de Segurança Cibernética

Utilizando os conceitos definidos pela norma IEC 62351 [25], os seguintes Domínios de Segurança, conforme apresentados na Figura 28, podem ser identificados na arquitetura do Setor Elétrico:

- Operação Crítica;
- Negócio Crítico;
- Corporativo; e
- Nacional.

Esses domínios podem ser físicos ou virtuais, são identificados, respectivamente, por cores diferentes (laranja, amarelo, verde e rosa), na Figura 28, e serão utilizados para propor, discutir ou avaliar as políticas de segurança específicas utilizadas no Brasil. O conceito de perímetro de cada domínio representa os limites, físicos ou abstratos, que delimitam um conjunto de ativos que se pretende manter no mesmo nível mínimo de segurança, idêntico para todos os ativos dentro do domínio.

Observa-se que a troca de informações de e para cada domínio de segurança é validada pelos requisitos de nível de segurança de cada domínio. Os domínios de segurança, por sua vez, compreendem ativos lógicos e físicos, que podem abranger mais de uma camada na arquitetura física e são resguardados por proteções lógicas e físicas comuns a cada camada.

O domínio de segurança de Operação Crítica, identificado pela cor laranja na Figura 28, aplica-se a todos os ativos diretamente relacionados à disponibilidade e à confiabilidade da infraestrutura de geração, transmissão, distribuição, consumo e conexão direta com os principais agentes do SIN. Este domínio pode ser utilizado para propor, auditar, documentar e avaliar a política de segurança utilizada pelas áreas operacionais dos agentes do SEB, em cada nível sob sua responsabilidade.

O domínio de segurança de Negócio Crítico, identificado pela cor amarela na Figura 28, é adotado em todos os ativos corporativos que suportam o funcionamento administrativo dos agentes a nível das instalações, mas que não são críticos para a confiabilidade e disponibilidade do sistema elétrico. Este domínio pode ser empregado para propor, auditar, documentar e avaliar a segurança cibernética dos domínios de TI das instalações da rede elétrica.

O domínio de segurança Corporativo, identificado pela cor verde na Figura 28, é aplicado a todos os ativos de apoio à gestão empresarial dos agentes do setor elétrico, externos às instalações elétricas, mas possivelmente conectados aos centros de controle, cuja segurança não é diretamente responsável pela confiabilidade e disponibilidade da rede elétrica.

Este domínio pode ser adotado como referência para propor, auditar, documentar e avaliar as políticas de segurança empregadas nas redes de TI.

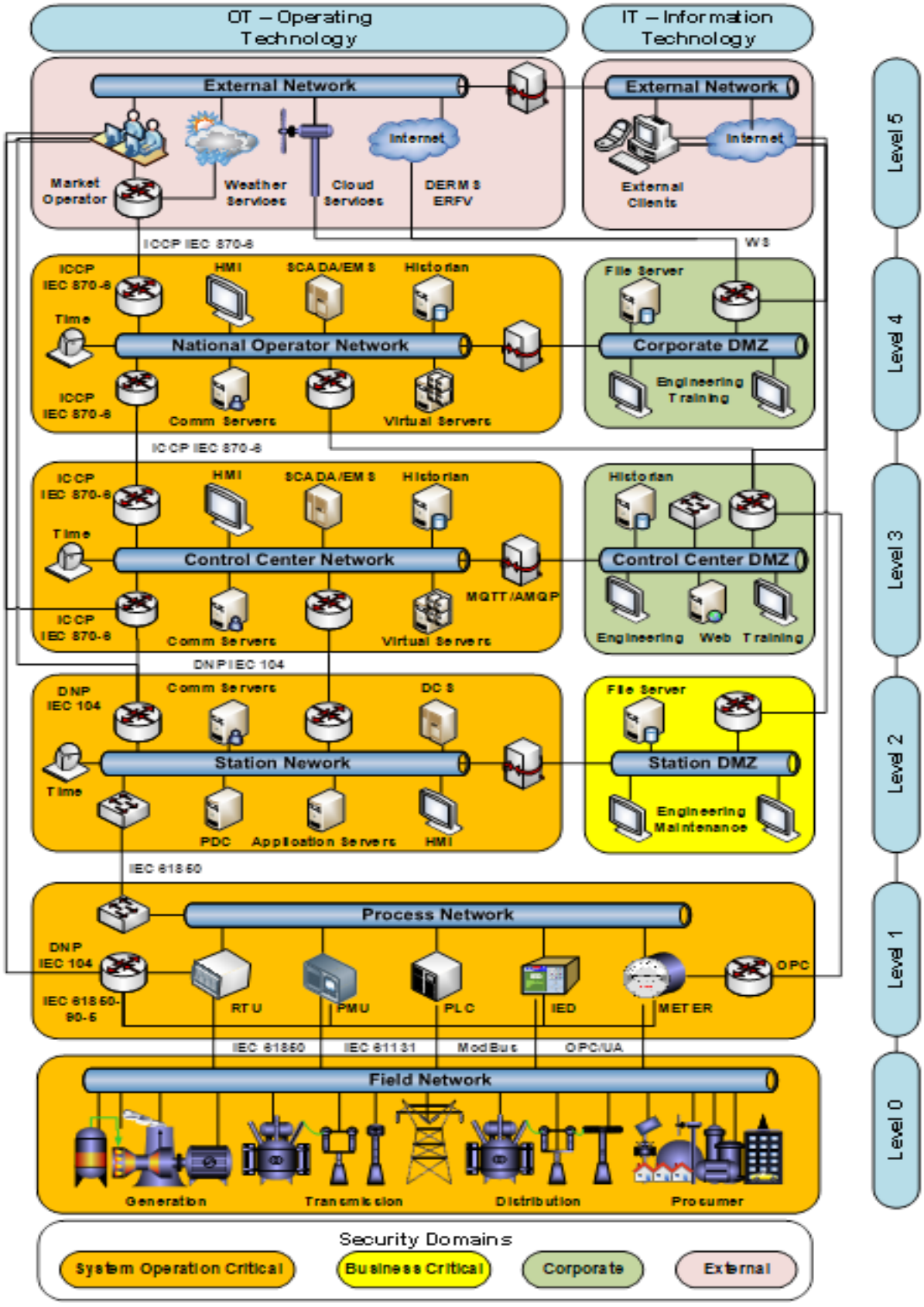
Por fim, o domínio de segurança Nacional, identificado pela cor rosa na Figura 28, adota-se em todos os ativos e entidades externas à Administração Pública, a nível nacional, para apoiar a operação empresarial e de mercado das corporações e a segurança das redes de infraestruturas críticas nacionais, que utilizam a comunicação via redes públicas ou privadas. Este domínio pode ser adotado para propor, auditar, documentar e avaliar as políticas de segurança a nível nacional, relacionadas às infraestruturas críticas e ao setor elétrico, em particular.

Destaca-se que os domínios de segurança são interligados verticalmente e horizontalmente, dentro e fora de cada agente do SIN, por meios de comunicação próprios e de terceiros.

5.3 Arquitetura de Comunicações

A Figura 29, abaixo, ilustra a composição característica de cada camada do modelo de arquitetura de ativos cibernéticos proposto para o SEB, com os ativos típicos de TI/TO e as interligações de TL normalmente utilizadas entre estas camadas, com alguns protocolos usuais padronizados para o setor.

Figura 29 – Arquitetura de Ativos Cibernéticos do Setor Elétrico



Fonte: Elaboração própria.

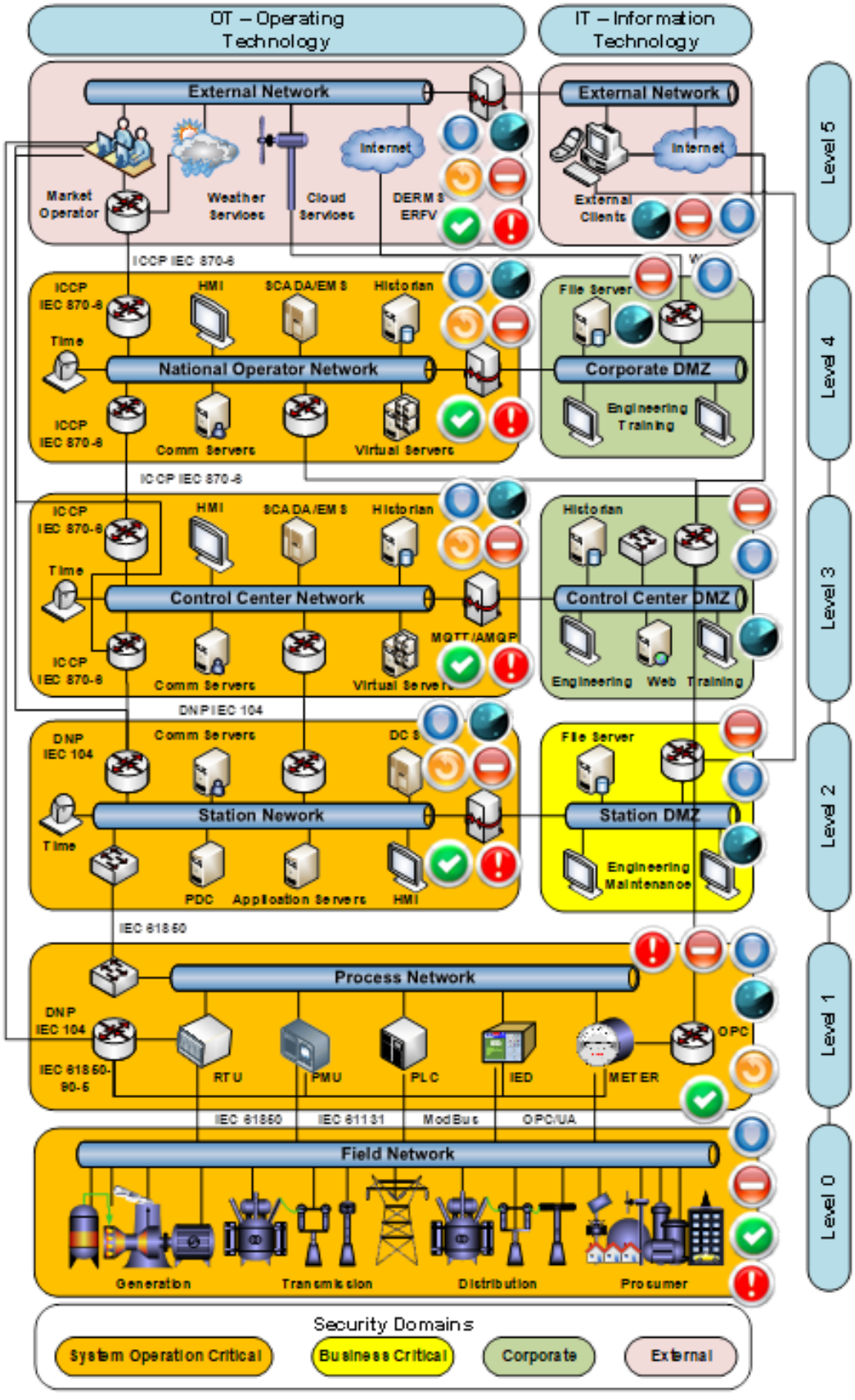
Note-se que, além da comunicação horizontal entre domínios de um mesmo nível e da comunicação vertical entre níveis adjacentes, é comum a comunicação direta entre níveis não adjacentes, mediante a utilização de protocolos abertos e públicos, o que aumenta a vulnerabilidade de toda a cadeia operacional e de gestão do SIN. Deste modo, é possível uma comunicação direta entre um agente externo e um ativo nos níveis inferiores da hierarquia, se aquele agente possuir as credenciais necessárias.

Além das políticas e dos controles comuns a cada domínio, esta arquitetura permite explicitar as contramedidas de proteção específicas dos ativos e domínios em cada camada, bem como as interligações entre domínios. A arquitetura pode ser utilizada para propor, auditar, documentar e avaliar as políticas de segurança para cada domínio e tipo de ativo de cada domínio e para as interligações entre as camadas e domínios, sem entrar nos detalhes construtivos dos domínios ou ativos, a critério dos agentes.

5.4 Políticas de Segurança

Utilizando a arquitetura do modelo PERA da Figura 29, acima, é possível propor, auditar, documentar e avaliar políticas (mínimas) recomendadas ou implementadas em cada camada da estrutura do SIN, selecionadas por um processo anterior de análise de riscos, conforme sugerido na Subseção 4.2. A Figura 30, a seguir, demonstra uma possível alocação de políticas de segurança, agnósticas quanto a tecnologias ou fornecedores, sugeridas para todas as camadas da hierarquia funcional do SIN, a partir da utilização das classes abstratas de políticas listadas na Tabela 2.

Figura 30 – Políticas de Segurança do Setor Elétrico



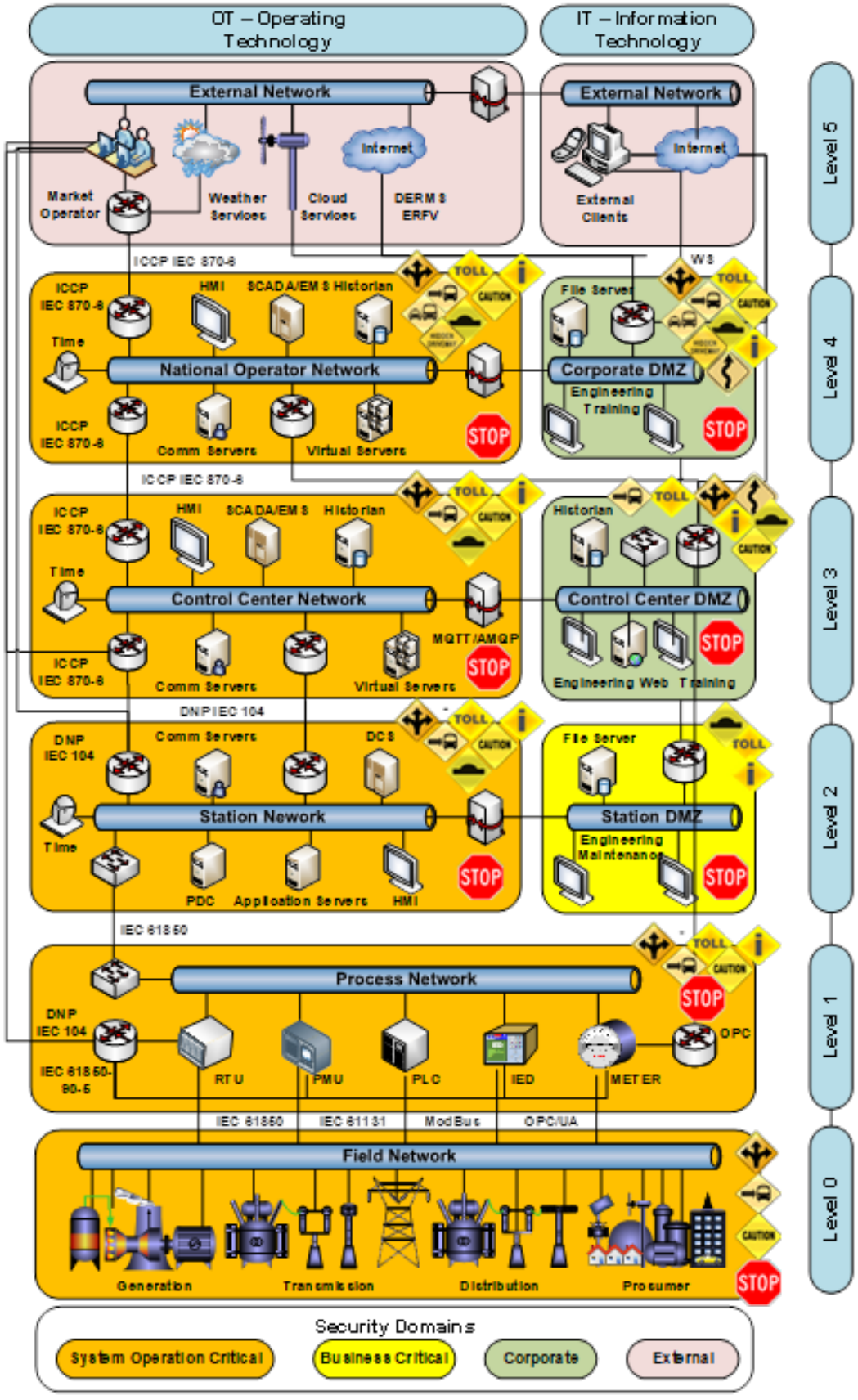
Fonte: Elaboração própria.

Esta arquitetura é apenas uma sugestão das possibilidades de políticas de segurança para cada camada e domínio da hierarquia funcional do SIN e deve ser precedida por uma análise de riscos (Subseção 4.2) para cada proposição de política, entre aquelas padronizadas. Assim, uma vez escolhidas estas políticas, é possível sugerir, auditar, documentar e avaliar os controles e as contramedidas propostas ou implementadas em cada camada e domínio de segurança do SIN.

5.5 Contramedidas de Segurança

Estabelecidas as políticas aplicáveis ao modelo PERA da Figura 30, é possível propor, auditar, documentar e avaliar os controles e contramedidas recomendadas ou implementadas em cada camada da estrutura do SIN, conforme sugerido na Subseção 4.4. Em seguida, a Figura 31 ilustra uma possível alocação destes controles, agnósticos quanto a tecnologias ou fornecedores, a partir dos ícones gráficos da Tabela 4, propostos para todas as camadas da hierarquia funcional do SIN e associados às classes abstratas de controles, apresentadas nesta tabela, para as políticas selecionadas. Essa representação é apenas conceitual, consistindo na sugestão de uma possível regulamentação aplicável ao SEB e de ferramentas de regulação, discussão e auditoria no que diz respeito à segurança cibernética do SIN.

Figura 31 – Arquitetura de Controle Cibernético do Setor Elétrico



Fonte: Elaboração própria.

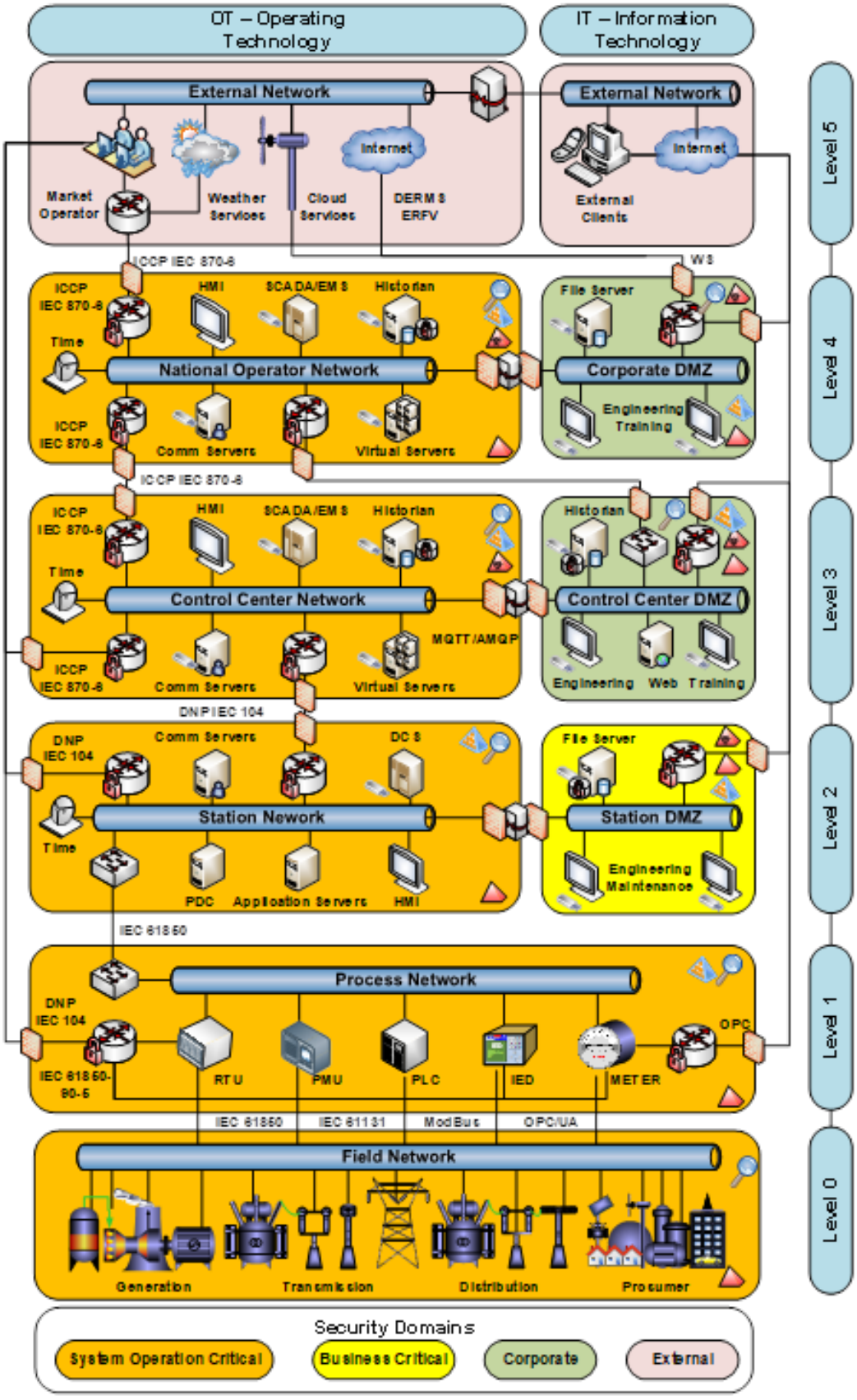
A partir dos símbolos da Figura 31, acima, e seguindo o padrão recomendado pela IEC 62351 [32], as contramedidas mínimas de segurança recomendadas para a arquitetura de ativos físicos do setor elétrico para os domínios de segurança definidos são descritas a seguir. Estas contramedidas e estes controles podem ser implementados utilizando soluções tecnológicas padronizadas ou especialmente desenvolvidas para o SEB, de escolha de cada agente.

5.6 Tecnologias de Segurança Cibernética

Como opção tecnológica para atender aos controles e às políticas regulamentados, os agentes do SEB podem optar por soluções disponíveis comercialmente ou desenvolvidas sob medida para cada ativo, domínio ou camada da arquitetura do SIN. Estas soluções também podem ser documentadas de forma padronizada, para cada camada e domínio do modelo PERA da Figura 30, objetivando facilitar a proposição, a auditoria, a documentação e a avaliação dos controles e das contramedidas implementados na estrutura do SIN, conforme sugerido na Subseção 4.5.

A Figura 32 ilustra uma possível alocação destas tecnologias, novamente agnósticas quanto aos fornecedores, mediante a utilização dos ícones gráficos da Tabela 5, sugeridos para todas as camadas da hierarquia funcional do SIN, associados às classes abstratas de tecnologias para os controles selecionados. Novamente, esta representação é apenas conceitual, como sugestão de uma possível implementação dos controles selecionados na subseção anterior e de ferramentas de regulação, auditoria e discussão com os agentes interessados na segurança cibernética do SIN.

Figura 32 – Tecnologias de Segurança Cibernética do Setor Elétrico



Fonte: Elaboração própria.

Para os ativos localizados nos domínios críticos da operação, as seguintes contramedidas mínimas de segurança são sugeridas, conforme ilustrado, anteriormente, na Figura 31.

- Restrições de tráfego para comunicação proibida (*Firewalls*) com entidades internas, como centros de controle de *backup*, subestações, usinas e usuários corporativos, bem como com entidades externas;
- Autenticação multifatorial ou respostas de desafio (Autenticações Fortes) em todos os servidores;
- Agrupamento administrativo de múltiplas redes privadas (Domínios) para os ativos em tempo real do centro de controle;
- Controle de acesso baseado em função (RBAC) para todos os ativos do centro de controle;
- Opções de segurança específicas dos protocolos utilizados para se conectar ao centro nacional, ao centro de controle de *backup*, às subestações e às usinas;
- Zonas desmilitarizadas (DMZ) para separar LANs de redes não confiáveis, principalmente para trocar dados com usuários corporativos e clientes externos;
- Dissimulação de informações para entidades não autorizadas (criptografia de dados), principalmente para historiadores;
- Segregação de tráfego (VPN) para proteger a comunicação com entidades internas; e
- Registro de eventos para auditoria (monitoramento) de interações com todos os ativos em tempo real.

Para os ativos localizados nos domínios críticos de negócio dos agentes e do ONS, as seguintes contramedidas mínimas de segurança são sugeridas, conforme ilustrado na Figura 31, acima.

- Restrições de tráfego para comunicação proibida (*Firewalls*) com entidades internas e externas, principalmente com o domínio em tempo real;
- Autenticação multifatorial ou respostas de desafio (autenticações fortes) em todos os servidores da DMZ do centro de controle;

- Agrupamento administrativo em múltiplas redes privadas (domínios) para os ativos da DMZ do centro de controle e da rede corporativa;
- Controle de acesso baseado em função (RBAC) para todos os ativos da DMZ do centro de controle e da rede corporativa;
- Opções de segurança nativas específicas dos protocolos utilizados para se conectar à rede corporativa e a clientes externos;
- Segregação de tráfego (VPN) para proteger a comunicação com entidades internas e externas;
- Registro e gravação de eventos para auditoria (monitoramento) de interações com todos os ativos da DMZ e do ambiente em tempo real; e
- Detecção e remoção de vírus.

Finalmente, para os ativos localizados nos domínios corporativos dos agentes e do ONS, as seguintes contramedidas mínimas de segurança são propostas, conforme apresentado, acima, na Figura 31

- Restrições de tráfego para comunicação proibida (*Firewalls*) com entidades externas, incluindo serviços meteorológicos, serviços em nuvem, DERMS, internet e clientes externos;
- Autenticação multifatorial ou respostas de desafio (autenticações fortes) em todos os servidores da DMZ corporativa;
- Agrupamento administrativo em múltiplas redes privadas (domínios) na DMZ corporativa;
- Controle de acesso baseado em função (RBAC) para todos os ativos da DMZ corporativa;
- Opções específicas de segurança dos protocolos utilizados para se conectar a clientes e entidades externas;
- Segregação de tráfego (VPN) para clientes externos que precisam acessar ativos corporativos de TI;
- Registro e gravação de eventos para auditoria (monitoramento) de todos os acessos internos e externos; e
- Detecção e remoção de vírus.

Ressalta-se que esta arquitetura é apenas uma sugestão das tecnologias de segurança aplicáveis a cada camada e domínio da hierarquia funcional do SIN, devendo ser selecionada pelos agentes para atender ao conjunto de contramedidas e políticas estabelecidas para o SEB, conforme as arquiteturas apresentadas da Figura 28 à Figura 32. De posse destas soluções, é possível propor, auditar, documentar e avaliar aquelas adotadas pelos agentes e implementadas em cada camada e domínio de segurança do SIN.

6. Conclusões

A segurança cibernética de cada instalação do SIN deve atender às diretrizes da Política Nacional de Segurança, às normas nacionais e aos procedimentos de rede do ONS e aos padrões de segurança nacionais, definidos pela ABNT, ou internacionais aplicáveis, da IEC, IEEE e NIST.

Recomenda-se que sejam definidos requisitos mínimos a partir de uma arquitetura de referência que descreva todas as visões comuns aos sistemas SCADA/EMS, utilizando, principalmente, os conceitos arquiteturais comuns às normas ISA99 [27] e IEC 62443 [26] ou os modelos do *National Institute of Standards and Technology* (NIST) [23][24], com o objetivo de manter uma abordagem consistente da segurança cibernética.

Em particular, sugere-se a adoção de uma abordagem de cima para baixo (*topdown*), iniciando pelo estabelecimento de uma estratégia sintonizada com as Estratégias Nacionais de Transformação Digital (Subseção 3.1) e de Segurança Cibernética (Subseção 3.2), desdobradas em políticas suportadas por uma análise de riscos específica para o SEB (parágrafo 4.2), de modo a resultar em uma série de controles de segurança (Subseção 4.4).

Destaca-se que este método permite que definições sucessivas sejam adotadas para a montagem do arcabouço regulatório de segurança cibernética para o Setor Elétrico Brasileiro, com a discussão pública da análise de riscos, culminando com as ações de auditoria nos controles e nas tecnologias empregadas (Subseção 4.5) pelos agentes do setor.

No Brasil, ações neste sentido estão sendo adotadas pela ANEEL, através da Consulta Pública nº 07/2021 [51], que visa obter subsídios para a Análise de Impacto Regulatório sobre a segurança cibernética no Setor Elétrico Brasileiro [52], com o objetivo de avaliar as possíveis intervenções regulatórias no tema, e pelo ONS [53] para estabelecer os controles mínimos de segurança cibernética a serem implementados pelos agentes e pelo ONS no Ambiente Regulado Cibernético (ARCiber) envolvendo

os centros de operação dos agentes; os equipamentos que participam da infraestrutura de envio ou recebimento de dados e voz para ambientes operativos do ONS ou para centros de operação de outros agentes; e o próprio ambiente operativo do ONS. Nota-se que medidas semelhantes estão sendo estudadas pelo ONS, com a finalidade de implementar adequações aos Procedimentos de Rede do SIN para instalações digitais.

Como política e estratégia nacionais, a proteção das infraestruturas críticas e, em particular, do setor elétrico deve ser considerada uma função estratégica de Estado, parte do arcabouço de Defesa Nacional e essencial para a manutenção da vida em sociedade. As corretas definições de políticas e estratégias de proteção e defesa, seguidas da implementação de uma estrutura funcional hierárquica de regulação, governança e fiscalização adequadas, são os requisitos para o sucesso. Pela complexidade e extensão continental do SEB, é necessário, contudo, um esforço conjunto entre o poder público, as instituições do setor elétrico, os setores privados, a Academia e a sociedade, objetivando a implementação de medidas efetivas de segurança cibernética e a conscientização de todos os cidadãos da necessidade de cumpri-las.

Referências

[1] SIQUEIRA, I. P. Rede de Infraestruturas Críticas – Análise de Desempenho e Riscos dos Setores de Energia, Petróleo, Gás, Água, Finanças, Logística e Telecomunicações, Editora Interciencia, Rio de Janeiro, 2013.

[2] SIQUEIRA, I. P. Cyber Security of Electrical Networks, Tutorial presented during the International Seminar of Smart Grids, Rio de Janeiro, 2018.

[3] SIQUEIRA, I. P. A Reliability-Centered Maintenance Approach to Cybersecurity of Protection and Automation Systems, Protection Automation and Control Conference, Slovenia, 2018.

[4] SIQUEIRA, I. P. Maintenance of Cybersecurity of Electrical Networks, Tutorial presented during the Relay Protect Conference, St. Petersburg, Russia, 2015.

[5] SIQUEIRA, I. P. Ensuring the Cybersecurity in the Power System, Contribution to the Roundtable on Cybersecurity, XXX, St. Petersburg, Russia, 2017.

[6] Castro, N.; Câmara, L.; Moszkowicz, M. A segurança cibernética e o setor elétrico, Disponível em: https://energia.aebroadcast.com.br/tabs/news/746/36467198. Acessado em: 22 de janeiro de 2021.

[7] Alves, V. *et al*. Segurança Cibernética e Políticas Públicas no Brasil, XI Simpósio de Excelência em Gestão e Tecnologia, 2014. Disponível em: https://www.researchgate.net/publication/275272400. Acessado em: 20 de março de 2021.

[8] GSI, Gabinete de Segurança Institucional da Presidência da República. Portaria GSI nº 2, de 8 de fevereiro de 2008.

[9] Souza, A. F. Segurança Cibernética: Política Brasileira e a Experiência Internacional, Dissertação de Mestrado, Universidade Católica de Brasília, Brasília, 2013.

[10] Presidência da República, Secretaria Geral, Subchefia para Assuntos Jurídicos. Decreto nº 9.573, de 22 de novembro de 2018.

[11] Presidência da República, Secretaria Geral, Subchefia para Assuntos Jurídicos. Decreto nº 9.637, de 26 de dezembro de 2018.

[12] Presidência da República, Secretaria Geral, Subchefia para Assuntos Jurídicos. Decreto nº 9.319, de 31 de março de 2018.

[13] ONS, Operador Nacional do Sistema Elétrico. Website, 2021. Disponível em: www.ons.org.br. Acessado em: 07 de abril de 2021.

[14] ABEEOLICA, Associação Brasileira de Energia Eólica. Website, 2021. Disponível em: http://abeeolica.org.br. Acessado em: 07 de abril de 2021.

[15] Presidência da República, Secretaria Geral, Subchefia para Assuntos Jurídicos. Decreto nº 10.222, de 5 de fevereiro de 2020.

[16] Presidência da República, Secretaria Geral, Subchefia para Assuntos Jurídicos. Decreto nº 10.569, de 9 de dezembro de 2020.

[17] Presidência da República, Secretaria Geral, Subchefia para Assuntos Jurídicos. Decreto nº 9 669, de 2 de janeiro de 2019.

[18] GCSCC, Global Cyber Security Capacity Centre; OAS, Organization of American States. Cybersecurity Capacity Review - Federative Republic of Brazil, Global Cyber Security Capacity Center, Organization of American States, Brasilia, 2019.

[19] Imagem de https://www.cert.br/csirts/brazil/. Acessada em: 07 de maio de 2019.

[20] CMM, Cybersecurity Capacity Maturity Model for Nations. Revised Edition. Disponível em: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition. Acessado em: 25 de fevereiro de 2018.

[21] Williams, T.J. The Purdue Enterprise Reference Architecture and Methodology (PERA), Institute for Interdisciplinary Engineering Studies Purdue University, West Lafayette, IN, 1990.

[22] NERC, North American Electric Reliability Corporation. CIP-002-5.1a: Cyber Security — BES Cyber System Categorization, NERC Critical Infrastructure Protection Standards, North American Electric Reliability Corporation, March 2019.

[23] NIST, National Institute of Standards and Technology. Special Publication 800-82, Revision 2, Guide to Industrial Control Systems (ICS) Security, Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems

(DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC), National Institute of Standards and Technology, May 2015.

[24] NIST, National Institute of Standards and Technology. Special Publication 800-125, Guide to Security for Full Virtualization Technologies, National Institute of Standards and Technology, January 2011.

[25] IEC, International Electrotechnical Commission. IEC 62351, Power systems management and associated information exchange - Data and communications security, International Electrotechnical Commission, Geneva, 2012.

[26] IEC, International Electrotechnical Commission. IEC 62443, Industrial communication networks - Network and system security, International Electrotechnical Commission, Geneva, 2009.

[27] ISA, International Society of Automation. ISA 99, Industrial Automation and Control Systems Security, International Society of Automation. Website, 2021. Disponível em: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99 Acessado em: 11 de abril de 2021.

[28] Amoroso, E. Cyber Attacks: Protecting National Infrastructure, Butterworth-Heinemann, 2012.

[29] SIQUEIRA, I. P. A Reliability-Centered Maintenance Approach to Cybersecurity of Protection and Automation Systems. Website, 2021. Disponível em: www.tecnix.com.br. Acessado em 20 de março de 2021.

[30] SIQUEIRA, I. P.; Hatziargyriou, N., ed. Electricity Supply Systems of the Future, Springer, Switzerland, 2021.

[31] ISO, International Organization for Standardization. ISO 27000 - Information technology - Security techniques - Information security management systems, International Organization for Standardization. Website, 2021. Disponível em: https://www.iso.org/standard/73906.html. Acessado em: 22 de maio de 2021.

[32] IEC, International Electrotechnical Commission. IEC 62351 - Power systems management and associated information exchange - Data and communications security, International Electrotechnical Commission. Disponível em: https://webstore.iec.ch/. Acessado em: 22 de maio de 2021.

[33] IEC, International Electrotechnical Commission. IEC 62443 - Industrial communication networks - Network and system security (Former ISA 99), International Electrotechnical Commission. Disponível em: https://webstore.iec.ch/. Acessado em: 22 de maio de 2021.

[34] CIGRE, International Council on Large Electric Systems. TB 427 - The Impact of Implementing Cyber Security Requirements using IEC 61850. Disponível em: https://e-cigre.org/. Acessado em: 22 de maio de 2021.

[35] CIGRE, International Council on Large Electric Systems. TB 317 - Security for Information Systems and Intranets in Electric Power Systems. Disponível em: https://e-cigre.org/. Acessado em: 22 de maio de 2021.

[36] CIGRE, International Council on Large Electric Systems. TB 419 - Treatment of Information Security for Electric Power Utilities (EPUs). Disponível em https://e-cigre.org/. Acessado em: 22 de maio de 2021.

[37] CIGRE, International Council on Large Electric Systems. TB 603 - Application and Management of Cybersecurity Measures for Protection and Control. Disponível em: https://e-cigre.org/. Acessado em: 22 de maio de 2021.

[38] CIGRE, International Council on Large Electric Systems. Framework for EPU operators to manage the response to a cyber-initiated threat to their critical infrastructure (Under development by CIGRE SC D2).

[39] NIST, , National Institute of Standards and Technology. SP800 - Framework for Improving Critical Infrastructure Cybersecurity (CSF – Cyber-security Framework), National Institute of Standards and Technology, disponível em https://www.nist.gov/publications, acessado em 22 de maio de 2021.

[40] IEEE, Institute of Electrical and Electronics Engineers; SSCP, Secure Scada Communication Protocol. Disponível em: https://www.ieee.org/publications/. Acessado em: 22 de maio de 2021.

[41] NERC, North American Electric Reliability Corporation; CIP, Critical Infrastructure Protection. Disponível em https://www.nerc.com/Pages/default.aspx. Acessado em: 22 de maio de 2021.

[42] ISA, International Society of Automation. ISA99 - Network and system security for industrial-process measurement and control, The International Society of

Automation. Disponível em: https://www.isa.org/standards-and-publications/isa-publications. Acessado em: 22 de maio de 2021.

[43] USDOE, USDHS, ES-C2M2. Electricity Subsector Cybersecurity Capability Maturity Model, Energy Sector Cybersecurity Framework Implementation Guidance, US Department of Energy, US Department of Homeland Security. Disponível em: https://www.energy.gov/. Acessado em: 22 de maio de 2021.

[44] ABNT, Associação Brasileira de Normas Técnicas. NBR ISO 31000, Gestão de riscos. Disponível em http://www.abnt.org.br/. Acessado em: 22 de maio de 2021.

[45] ABNT, Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27001: 2019 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação. Disponível em: http://www.abnt.org.br/. Acessado em: 22 de maio de 2021.

[46] Lucszo, Z. *et al*. Securing Electricity Supply in the Cyber Age: Exploring the Risks of Information and Communication Technology in Tomorrow's Electricity Infrastructure. Disponível em: https://www.springer.com/gp/book/9789048135936. Acessado em: 22 de maio de 2021.

[47] Sorebo, G.; Echols, M. Smart Grid Security: An End-to-End View of Security in the New Electrical Grid. Disponível em: https://www.routledge.com/Smart-Grid-Security-An-End-to-End-View-of-Security-in-the-New-Electrical/Sorebo-Echols/p/book/9781439855874. Acessado em: 22 de maio de 2021.

[48] Peltier, T. Information Security Risk Analysis. Disponível em: http://www.nojutso.com/downloads/diplomado/ISRA%20Peltier.pdf. Acessado em: 22 de maio de 2021.

[49] Lewis, T. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Disponível em: https://www.wiley.com/en-us/Critical+Infrastructure+Protection+in+Homeland+Security%3A+Defending+a+Networked+Nation%2C+3rd+Edition-p-9781119614531. Acessado em: 22 de maio de 2021.

[50] Krutz, R. L. Securing Scada Systems. Disponível em: https://www.wiley.com/en-us/Securing+SCADA+Systems-p-9780764597879. Acessado em: 22 de maio de 2021.

[51] ANEEL, Agência Nacional de Energia Elétrica. Consulta Pública ANEEL nº 07/2021. Obter subsídios para a Análise de Impacto Regulatório - AIR sobre a segurança cibernética no Setor Elétrico Brasileiro. Disponível em: www.aneel.gov.br/consultas-publicas?p_p_id=participacaopublica_WAR_participacaopublicaportlet&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_pos=1&p_p_col_count=2&_participacaopublica_WAR_participacaopublicaportlet_situacao=1. Acessado em 29 de abril de 2021.

[52] ANEEL, Agência Nacional de Energia Elétrica. Análise de Impacto Regulatório (AIR) sobre segurança Cibernética no Setor Elétrico Brasileiro, Relatório de Análise de Impacto Regulatório nº 2/2021-SRT-SGI-SRD-SRG/ANEEL. Disponível em: https://www.aneel.gov.br/consultas-publicas?p_p_id=participacaopublica_WAR_participacaopublicaportlet&p_p_lifecycle=2&p_p_state=normal&p_p_mode=view&p_p_cacheability=cacheLevelPage&p_p_col_id=column-2&p_p_col_pos=1&p_p_col_count=2&_participacaopublica_WAR_participacaopublicaportlet_ideDocumento=41967&_participacaopublica_WAR_participacaopublicaportlet_tipoFaseReuniao=fase&_participacaopublica_WAR_participacaopublicaportlet_jspPage=%2Fhtml%2Fpp%2Fvisualizar.jsp. Acessado em: 29 de abril de 2021.

[53] ONS, Operador Nacional do Sistema Elétrico. Rotina Operacional RO-CB.BR.01, Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético, Manual de Procedimentos da Operação, Módulo 5 - Submódulo 5.13, Rio de Janeiro, julho de 2021.

Grupo de Estudos do Setor elétrico
Gesel

Toda a produção acadêmica e científica do GESEL está disponível no site do Grupo, que também mantém uma intensa relação com o setor através das redes sociais Facebook e Twitter.

Destaca-se ainda a publicação diária do IFE - Informativo Eletrônico do Setor Elétrico, editado deste 1998 e distribuído para mais de 10.000 usuários, onde são apresentados resumos das principais informações, estudos e dados sobre o setor elétrico do Brasil e exterior, podendo ser feita inscrição gratuita em http://cadastro-ife.gesel.ie.ufrj.br

GESEL – Destacado think tank do setor elétrico brasileiro, fundado em 1997, desenvolve estudos buscando contribuir com o aperfeiçoamento do modelo de estruturação e funcionamento do Setor Elétrico Brasileiro (SEB). Além das pesquisas, artigos acadêmicos, relatórios técnicos e livros – em grande parte associados a projetos realizados no âmbito do Programa de P&D da Aneel – ministra cursos de qualificação para as instituições e agentes do setor e realiza eventos – work shops, seminários, visitas e reuniões técnicas – no Brasil e no exterior. Ao nível acadêmico é responsável pela área de energia elétrica do Programa de Pós-Graduação em Políticas Públicas, Estratégias e Desenvolvimento do Instituto de Economia (PPED) do Instituto de Economia da UFRJ

ISBN: 978-65-86614-28-2

SITE: gesel.ie.ufrj.br

FACEBOOK: facebook.com/geselufrj

TWITTER: twitter.com/geselufrj

E-MAIL: gesel@gesel.ie.ufrj.br

TELEFONE: (21) 3938-5249
(21) 3577-3953

Scan me

Versão Digital

ENDEREÇO:

UFRJ - Instituto de Economia.
Campus da Praia Vermelha.

Av. Pasteur 250, sala 226 - Urca.
Rio de Janeiro, RJ - Brasil.
CEP: 22290-240