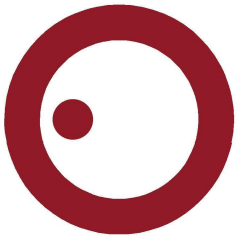


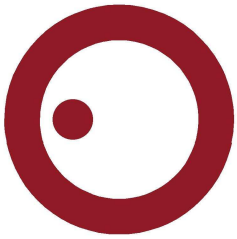
escola superior de tecnologia e gestão
instituto politécnico de leiria

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado de Cibersegurança e Informática Forense

ROTEIRO DE CAPACIDADES MINÍMAS DE CIBERSEGURANÇA NO SECTOR ENERGÉTICO

MARCO ANTÓNIO VITORINO PASSAGEM

Leiria, Setembro de 2023



escola superior de tecnologia e gestão
instituto politécnico de leiria

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado de Cibersegurança e Informática Forense

ROTEIRO DE CAPACIDADES MINÍMAS DE CIBERSEGURANÇA NO SECTOR ENERGÉTICO

MARCO ANTÓNIO VITORINO PASSAGEM
Número: 2210256

Projeto realizado sob orientação do Professor Ricardo Jorge Pereira Gomes (ricardo.p.gomes@ipleiria.pt).

Leiria, Setembro de 2023

AGRADECIMENTOS

Agradeço ao meu orientador Ricardo Jorge Pereira Gomes a ajuda e apoio dado na realização da tese e na filtração da informação a usar na mesma. Sem a orientação e ajuda do professor Ricardo Gomes não seria possível ter a qualidade apresentada nesta tese.
Agradeço ainda à minha família pelo apoio dado e por encorajarem-me, à minha namorada que me ajudou imenso e que esteve sempre presente até nas minhas maiores dificuldades e aos meus amigos por me incentivarem a melhorar cada vez mais e por acreditarem em mim.

RESUMO

A indústria energética é um sector critico para a sociedade, sendo que múltiplos serviços críticos dependem do seu bom funcionamento como, por exemplo, hospitais, telecomunicações ou apenas a população em geral e as suas necessidades. Devido a esta abrangência, aumentam também os riscos de ataques e por conseguinte o impacto caso estes sejam bem sucedidos. Devido ao perigo destes ataques é preciso assegurar que estes serviços são devidamente protegidos contra ciberataques, sendo no caso desta tese focada no sector energético. Caso os ataques sejam bem sucedidos, podem ter resultados catastróficos em termos de danos materiais e humanitários.

Para este efeito, este projeto visa a criação de um roteiro de capacidades mínimas para o sector energético, sendo este um sector extremamente critico e desastroso caso falhe. Para atingir o objetivo de criar o roteiro, primeiro foi pesquisado sobre a cibersegurança e as suas componentes para contextualizar sobre o que já é utilizado para a garantir.

Foi necessário descobrir que normas estão associadas aos sectores críticos e especialmente os usados no sector energético. Para isto foram realizadas várias pesquisas sobre as entidades reguladores do sector energético, tanto nacionais como europeias. Foi pesquisado como funciona o sector, tecnologias usadas no mesmo para monitorizar, prevenir e detetar falhas de segurança em termos da grelha energética e tecnologias já aplicadas e/ou que possam ser aplicadas para garantir a segurança.

Foram descobertos roteiros comparativos aplicadas a áreas específicas da indústria energética ou a sectores críticos, vulnerabilidades já existentes na indústria e soluções para as mesmas. Tendo realizado estas pesquisas, foi possível criar o roteiro, tendo este como base o roteiro de capacidades mínimas do CNCS, para que qualquer empresa do sector energético melhore as suas capacidades de cibersegurança, podendo ter uma melhor capacidade de detetar e prevenir ataques.

ABSTRACT

The energy industry is a critical sector for society, with multiple critical services depending on its proper functioning such as hospitals, telecommunications or just the general population and its needs. Due to this scope, the risks of attacks also increase and therefore the impact if they are successful. Due to the danger of these attacks, it is necessary to ensure that these services are properly protected against cyberattacks, in the case of this thesis focused on the energy sector. If the attacks are successful, they can have catastrophic results in terms of material and humanitarian damage.

For this effect, this project aims to create a roadmap of minimum capacities for the energy sector, which is an extremely critical and disastrous sector if it fails. In order to achieve the objective of creating the roadmap, cybersecurity and its components were first researched to contextualize what is already used to guarantee it.

It was necessary to discover which standards are associated with critical sectors and especially those used in the energy sector. For this, several researches were carried out on the regulatory authorities of the energy sector, both national and European. It was researched how the sector works, technologies used in it to monitor, prevent and detect security failures in terms of the energy grid, and technologies already applied and/or that can be applied to guarantee security.

Comparative roadmaps were discovered applied to specific areas of the energy industry or to critical sectors, existing vulnerabilities in the industry and solutions for these vulnerabilities. Having carried out these researches, it was possible to create the roadmap, based on the CNCS minimum capabilities roadmap, so that any company in the energy sector improves its cybersecurity capabilities, being able to have a better ability to detect and prevent attacks.

ÍNDICE

Agradecimentos i

Resumo iii

Abstract v

Índice vii

Lista de Figuras xiii

Lista de Abreviaturas xv

1 Introdução 1

2 Conceitos Relacionados 5

2.1 Cibersegurança . . . 5

2.1.1 Segurança de dispositivos . . . 5

2.1.2 Segurança de rede . . . 6

2.1.3 Segurança de informação . . . 9

2.1.4 Segurança aplicacional . . . 9

2.1.5 Segurança operacional . . . 11

2.1.6 Plano de recuperação de desastre e continuidade de negócio . 12

2.1.7 Gestão de Informações e Eventos de Segurança . . . 12

2.1.8 *Software* de deteção de anomalias . . . 13

2.1.9 *Smart Grids* . . . 13

2.1.10 Sistemas SCADA . . . 14

2.1.11 *Wide Area Monitoring System* . . . 14

2.2 Barreiras atuais para o melhoramento da segurança no sector elétrico 15

2.3 Tecnologia Operacional . . . 16

2.4 Gestão, monitorização, proteção e controlo da rede elétrica . . . 19

2.5 O que são normas de cibersegurança e quais existem . . . 20

2.6 O que é o sector energético e quais as suas entidades reguladoras . . 23

2.7 *Standards* . . . 25

2.7.1 ISO 9001 . . . 25

2.7.2 ISO 14001 . . . 26

2.7.3 ISO 50001 . . . 26

2.7.4 ISO 45001 . . . 27

2.7.5 ISO 27001 28
2.7.6 ISO 27019:2017 34

3 Trabalhos Relacionados 37
3.1 Roteiro para Capacidades Mínimas de Cibersegurança 37
3.2 *Guide to Industrial Control Systems Security* 38
3.3 *Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry* 39
3.4 *Framework for Improving Critical Infrastructure Cybersecurity* . . . 40
3.5 *Roadmap for Photovoltaic Cyber Security* 41
3.6 Cibersegurança numa rede de energia: estado da arte 43
3.7 *Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources* 44
3.8 *A "Review" on Cybersecurity in Smart Local Energy Systems: Requirements, Challenges, and Standards* 45
3.9 *Cybersecurity and the Smarter Grid* 47
3.10 *Research on Cybersecurity Strategy and Key Technology of the Wind Farms' Industrial Control System* 47
3.11 *Operational Technology Cybersecurity for Energy Systems* 48

4 Análise 49
4.1 Roteiro para Capacidades Mínimas de Cibersegurança 49
4.2 *Guide to Industrial Control Systems Security* 49
4.3 *Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry* 51
4.4 *Framework for Improving Critical Infrastructure Cybersecurity* . . . 51
4.5 *Roadmap for Photovoltaic Cyber Security* 52
4.6 Cibersegurança numa rede de energia: estado da arte 52
4.7 *Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources* 53
4.8 *A Review on Cybersecurity in Smart Local Energy Systems: Requirements, Challenges, and Standards* 53
4.9 *Cybersecurity and the Smarter Grid* 54
4.10 *Research on Cybersecurity Strategy and Key Technology of the Wind Farms' Industrial Control System* 54
4.11 *Operational Technology Cybersecurity for Energy Systems* 54

5 Metodologia 55

6 Proposta 59
6.1 Fase 1 . . . 62
6.1.1 Apresentação de caso de estudo do negócio . . . 62
6.1.2 Envolvimento e colaboração das várias entidades da empresa 63
6.1.3 Exemplo de arquitetura de alto nível . . . 63
6.1.4 Diagrama estrutural da empresa e recolha de ativos . . . 65
6.1.5 Identificação de criticidade de ativos e criação de políticas de segurança . . . 65
6.1.6 Definir políticas e procedimentos de segurança específicos para o ICS . . . 66
6.2 Fase 2 . . . 67
6.2.1 Arquitetura de Referência . . . 67
6.2.2 Descobrimento de ativos e monitorização . . . 69
6.2.3 Recolha de dados e a sua inventariação . . . 69
6.2.4 Identificação de ativos, a sua análise e a criação de linha base 70
6.2.5 Melhoria e adaptação da arquitetura de referência . . . 70
6.2.6 Implementação de sistema de recolha e armazenamento do fluxo de tráfego . . . 72
6.2.7 Instalação de *Phasor Measurement Units* . . . 72
6.2.8 Infraestrutura de medição avançada . . . 72
6.2.9 Inventariação de ativos / produção de um mapa de rede . . . 73
6.2.10 Recolha centralizada de registos . . . 74
6.2.11 Segurança de dados . . . 75
6.2.12 Criação de instrumentos de correção ou mitigação de incidentes 75
6.2.13 Estabelecimento de conformidade com a legislação aplicável . 76
6.2.14 Estabelecimento de conformidade com normas aplicáveis à área de atividade . . . 77
6.2.15 Criação de política de uso aceitável . . . 77
6.2.16 Tecnologia de proteção para equipamentos de OT e IT . . . 78
6.2.17 Manutenção de dispositivos . . . 79
6.3 Fase 3 . . . 80
6.3.1 Instalação de PDCs . . . 80
6.3.2 Instalação do Sistema SCADA . . . 80
6.3.3 Instalação do *Energy Management System* . . . 81
6.3.4 Instalação da *firewall* . . . 81
6.3.5 Segregação da rede . . . 83
6.3.6 Instalação e configuração de mecanismos de monitorização . . 86
6.3.7 Definição de procedimentos de operação . . . 86

6.3.8 Instalação e configuração de aplicações de monitorização em dispositivos . . . 88
6.3.9 Auditoria de segurança e Bases de Dados . . . 88
6.3.10 Instalação e configuração de controlo de acessos *web* . . . 89
6.3.11 Proteção e gestão de equipamentos . . . 89
6.3.12 *Hardening* das configurações . . . 89
6.3.13 Processos de deteção . . . 90
6.3.14 Instalação e configuração de um *Security Information and Event Management* . . . 91
6.3.15 Automação da distribuição energética . . . 92
6.4 Fase 4 . . . 92
6.4.1 Higiene e aplicação de *patches* de cibersegurança . . . 93
6.4.2 Criação de exercícios de segurança . . . 93
6.4.3 Criação de *playbooks* para ameaças mais comuns . . . 94
6.4.4 Processos de comunicação de incidentes . . . 95
6.4.5 Plano de resposta a incidentes . . . 95
6.4.6 Plano de comunicação e formação interna . . . 96
6.4.7 Criação de modelos de ameaças . . . 97
6.4.8 Planos de contingência para sistemas de energia . . . 98
6.4.9 Adoção de *standards* do sector . . . 98
6.4.10 Plano de restauro de sistemas . . . 99
6.5 Fase 5 . . . 100
6.5.1 Instalação de WAMS . . . 100
6.5.2 Instalação de um sistema de deteção de anomalias para ICS . . . 101
6.5.3 Plano de continuidade de negócio . . . 101
6.5.4 Aprovação e implementação de SOC . . . 102
6.5.5 Auditoria de segurança . . . 103
6.5.6 Realização de melhorias . . . 103
6.5.7 Participação em exercícios de cibersegurança . . . 103
6.5.8 Participação externa . . . 103
6.5.9 Protocolos de colaboração . . . 104

7 Conclusões 105

Bibliografia 107

Declaração 111

LISTA DE FIGURAS

Figura 1 Estrutura do documento 4
Figura 2 Arquitetura de Gestão de Ativos 40
Figura 3 Projetos financiados pelo departamento de Energia dos EUA por área 42
Figura 4 Segurança para Recursos de Energia Distribuída usando comunicações IEC 61850 e IEC 62351 43
Figura 5 Comparação dos Roteiros 50
Figura 6 Processos para obtenção da cibersegurança em sistemas fotovoltaicos descritos 52
Figura 7 Fases da proposta do roteiro 59
Figura 8 Função e Identificadores Únicos de Categorias 61
Figura 9 Arquitetura de Alto Nível 64
Figura 10 Arquitetura de Referência 67
Figura 11 Exemplo de uma arquitetura com várias *firewalls* e DMZ's . 71
Figura 12 Exemplo de uma arquitetura com *firewall* com uma DMZ entre a rede empresarial e a rede de controlo 84
Figura 13 Exemplo de uma arquitetura com *firewalls* pares entre a rede empresarial e a rede de controlo 85

LISTA DE ABREVIATURAS

ACER	Agency for the Cooperation of Energy Regulators.
AGC	Automatic generation control.
CEER	Council of European Energy Regulators.
CNCS	Centro Nacional de Cibersegurança.
DCS	Distributed control system.
DER	Distributed energy resources.
DMZ	Demilitarized Zone.
EMS	Energy Management System.
EPP	Endpoint protection platform.
GUI	Graphical User Interface.
HIDS	Host-based intrusion detection system.
IAM	Identity and Access Management.
ICCP	Intercontrol Center Communication Protocol.
ICS	Industrial control systems.
ICS-WF	Wind farm industrial control systems.
IDS	Intrusion Detection Systems.
IED	Inteligent electronic devices.
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos.
IOC	Indicadores de compromisso.
IoT	Internet of Things.

IPS	Intrusion Prevension Systems.
ISO	International Organization for Standardization.
IT	Informational Technology.
NIST	National Institute of Standards and Technology.
OT	Operational Technology.
PDC	phasor data concentrators.
PLC	Programmable logic controller.
PMU	Phasor measurement unit.
RBAC	Role-based access control.
RTU	Remote terminal unit.
SCADA	supervisão e aquisição de dados.
SCPSE	Security-Oriented Cyber-Physical State Estimation.
SGSI	Sistema de Gestão de Segurança de Informação.
SIEM	Security Information and Event Management.
SOAR	Security orchestration, automation and response.
SOC	Security Operations Center.
SSL	Secure Sockets Layer.
TIC	Tecnologias de informação e comunicação.
VPN	Virtual Private Network.
WAMS	Wide Area Monitoring System.

1

INTRODUÇÃO

Diversas áreas como a de transportes, energia e saúde, telecomunicações, finanças, segurança, processos democráticos, espaço e defesa dependem muito de redes e sistemas de informação que estão cada vez mais interligados. Com o aumento desta interconexão e da Internet aumentaram também os riscos de ciberataques e de atores mal-intencionados causarem variadas disrupções em diversos sectores.

Este cenário de ameaças é aumentado por tensões geopolíticas sobre a Internet aberta e global e sobre o controlo de tecnologias em toda a cadeia de fornecimento. Isto leva que os ataques maliciosos a infraestrutura crítica seja considerado um grande risco global. Segundo a Comissão Europeia, foram detetados quase 450 incidentes de cibersegurança em 2019 envolvendo infraestruturas críticas europeias, como finanças e energia.

De acordo com Jay Johson [1], em dezembro de 2015, um ciberataque na Ucrânia deixou 225.000 pessoas sem energia. Segundo Elise Vincente e publicado pelo Jornal LeMonde [2], com o início da guerra na Ucrânia foi visto um aumento enorme nos ciberataques e particularmente a estruturas críticas, nomeadamente hospitais, telecomunicações, produção de energia e relacionadas com o tratamento de água, sendo que desde o início da guerra os ciberataques na comunidade europeia aumentaram 46,5%.

Foi apurado pela *Blackkite* [3], empresa de desenvolvimento de soluções de cibersegurança, que:

- 25% do setor energético é altamente suscetível a um ataque de *ransomware*;
- 77% do setor energético tem pelo menos um roubo de credenciais nos últimos 90 dias;
- 28% do subsetor de energia, petróleo, é altamente vulnerável a um ataque de *ransomware*;
- 49% do setor energético tem uma vulnerabilidade crítica devido a sistemas desatualizados;

- 74% das empresas de energia não implantaram as configurações necessárias para evitar ataques de falsificação de correio eletrónico;

Isto implica que bastantes empresas do sector energético estão suscetíveis a ciberataques ou sem capacidades adequadas para se defenderem dos mesmos. Segundo um estudo sobre os índices do *S&P Dow Jones* [4], o sector energético representa 5,32% do peso nas empresas *S&P 500* sendo que é a segunda indústria mais concentrada do índice. Isto indica haver menos empresas a operar no sector comparativamente com o resto do sector, pendendo significar consequências maiores para os consumidores caso haja um ataque cibernético que inutilize os serviços.

Uma vez que é um dos sectores com menos competição, por ser mais centralizada, cada empresa terá um grande leque de clientes. Por este motivo uma falha de serviços de uma dessas empresas irá afetar um número grande de clientes, podendo ter consequências graves para os mesmos.

Devido a estes ataques é preciso assegurar que as estruturas críticas estão devidamente protegidas contra estes ataques, pois caso sejam afetadas os resultados podem ser catastróficos em termos de danos materiais e humanitários.

Para este meio, este projeto terá como objetivo a criação de um roteiro de capacidades mínimas para o sector energético, sendo este um sector extremamente critico e desastroso caso falhe.

Este roteiro irá permitir que qualquer empresa deste sector possa ter uma perceção adequada de cibersegurança seguindo o roteiro, mostrando passos a tomar, métodos a seguir pelos funcionários e ferramentas a utilizar pelas várias empresas do sector.

Este roteiro tem como base o roteiro de capacidades mínimas de cibersegurança criado pelo Centro Nacional de Cibersegurança de Portugal, onde são adicionadas várias peças especificas para o sector energético.

Este documento é composto pelos seguintes capítulos:

- Introdução, onde é introduzido trabalho, a audiência alvo, contexto e formato do mesmo;
- Conceitos relacionados, onde são introduzidos os conceitos e informações necessárias para contextualizar e ter um melhor entendimento do documento
- Trabalhos realizados, onde é feita a descrição dos trabalhos mais significativos analisados para a realização do documento;

- Análise, onde é feito uma análise dos trabalhos mencionados no capítulo anterior, onde é explicado que partes destes trabalhos foram usadas e a razão da escolha dos mesmos.
- Metodologia, onde é descrito o método usado para efetuar a pesquisa e redação do documento e a razão dos documentos selecionados.
- Proposta, onde é feito o detalhe da proposta que este documento se compromete, a redação do roteiro de capacidades mínimas de cibersegurança para o sector energético.
- Conclusão, onde são retiradas conclusões das pesquisas realizadas, do conhecimento obtido, dificuldades sentidas e trabalho futuro.

Na Figura 1 encontra-se um resumo da estrutura do documento realizado. Para o desenvolvimento do roteiro de capacidades mínimas de cibersegurança, haverá uma progressão da empresa, dividido por 5 fases. Estas fases darão à empresa mais segurança contra intrusões, uma troca de informações segura entre parceiros e uma capacidade de se reconfigurar para não permitir a falha de serviços. Além dessas capacidades, ela também conseguirá monitorizar intrusões, analisar dados analíticos e responder ativamente, guardando esses dados para uma futura análise ou para determinar atacantes, podendo fazer alterações para manter uma cibersegurança continua.

Figura 1: Estrutura do documento

2

CONCEITOS RELACIONADOS

Este capítulo irá enfatizar os conceitos relacionados ao roteiro de cibersegurança, dando uma introdução a para que passa existir um maior entendimento sobre os mesmos, o que irá permitir ao leitor obter o conhecimento necessário para ler claramente o roteiro e ter uma ideia contextualizada sobre os tópicos apresentados.

2.1 CIBERSEGURANÇA

Segundo a Kaspersky [5], a cibersegurança é a proteção de dispositivos móveis, computadores, servidores, redes de *internet* e outros sistemas eletrónicos, de ataques maliciosos.

Todos os tópicos seguintes são pertinentes para uma empresa do sector energético, pois esta irá ter sempre uma rede onde está integrada, com dispositivos ligados a esta, com *software* e aplicações proprietárias para a gestão da mesma, terá sempre que fazer o tratamento de dados e o seu armazenamento, terá colaboradores que terão que ser educados relativamente às boas práticas de segurança e um plano de recuperação de desastres, sendo que os serviços que esta fornece não podem ser parados, ao poderem afetar grande numero da população.

A cibersegurança pode ser subdivida em vários segmentos, cada um importante separadamente, e devem ser considerados em conjunto. Os segmentos apresentados nesta secção são segundo a Kaspersky [5], empresa de cibersegurança reconhecida mundialmente.

2.1.1 *Segurança de dispositivos*

Segurança de dispositivos prevê proteger todos os dispositivos informáticos da empresa de ataques maliciosos, independentemente se estes são dispositivos moveis, computadores, servidores ou de rede.

Segurança de dispositivos e plataformas de proteção de dispositivos funciona examinando registos, processos e sistemas para tentar encontrar atividades suspeitas ou maliciosas. A empresa pode instalar um Endpoint Protection Platform (EPP) para impedir que atacantes usem ferramentas para se infiltrar nos seus sistemas e comprometê-los. Um EPP pode ser usado em conjunto com outras ferramentas de deteção e monitorização para detetar comportamentos suspeitos e prevenir ataques antes que estes ocorram.

Esta proteção permite que a empresa realize uma gestão centralizada, ao qual a empresa pode conectá-la à sua rede. Esta permite que os administradores da empresa monitorizem, investiguem e respondam a possíveis ameaças cibernéticas. Esta abordagem pode ser local, na nuvem ou híbrida. O *software* de segurança de dispositivos normalmente inclui estes elementos:

- *Machine learning* detetar ameaças de *zero-day*;
- *Firewall* integrada para evitar ataques de redes;
- *Gateway* de endereço eletrónico para proteção contra tentativas de engenharia social;
- Proteção contra ameaças internas de dentro da empresa, maliciosas ou acidentais;
- Proteção antivírus e *antimalware* avançada para detetar e remover malware e outros *softwares* maliciosos em dispositivos e sistemas em operação
- Segurança proativa para facilitar a navegação segura na *web*
- Encriptação de dispositivos, correio eletrónico e de disco para proteção contra exfiltração de dados

Uma segurança de rede robusta permite proteger a rede contra várias ameaças, sendo esta como por exemplo *virus, worms, trojan, spyware, adware* ou *ransomware*. Todas estas ameaças podem comprometer a rede, como comprometer ou roubar dados, contas, *software* entre outros.

2.1.2 *Segurança de rede*

Segundo [6], pertencendo à empresa Checkpoint, a segurança de rede visa a proteção da rede interna da empresa, que liga os vários ativos informáticos da mesma, vigiando para que esta não seja comprometida.

Para proteção da rede existem várias proteções já implementadas, tanto em *hardware* como *software*. Estas podem ser usadas em conjunto ou apenas parte delas, sendo que devem usadas aquelas que façam sentido, ou que a empresa tenha capacidade de implementar. Serão expostas algumas soluções para proteção da rede.

Uma das soluções apresentadas, refere-se a *Firewalls* que permitem controlar o tráfego que sai e entra nas redes com regras de segurança por definição ou configuráveis. Com a definição das regras de segurança, estas permitem filtrar o tráfego indesejado e o tráfego diário esperado. É um método usado por todo o tipo de empresas, e com a introdução de *firewalls* de próxima geração, que permitem aprender que tráfego é esperado e que tráfego pode ser malicioso, por conseguirem observar o conteúdo de cada pacote de rede, há um maior foco em bloquear *malware* e aplicações que geram tráfego malicioso.

Para além desta solução pode ser aplicada a segmentação da rede, que permite definir segmentos de rede onde ativos partilham funções, riscos ou papeis em comum na empresa. Com esta segmentação, há um maior controlo das áreas de rede, permitindo uma maior proteção de dados sensíveis e que cada funcionário só tenha acesso ao segmento de rede que lhe permita desenvolver as suas atividades. Permite também criar zonas desmilitarizas (DMZ's) aonde apenas os servidores públicos estão expostos para o exterior, não permitindo ter visibilidade para a rede interna da empresa. Estes fatores permitem uma maior segurança e maior controlo de acessos.

Deve existir um controlo de acessos, definido pelas pessoas ou grupo de pessoas e dispositivos com acesso às aplicações de rede e sistemas, permitindo negar acessos sem autorização e ameaças. Integrações com produtos de Gestão de Acessos e Identidades - *Identity and Access Management* (IAM) identificam o utilizador e políticas de Controlo de Acessos Baseados em Funções - *Role Based Access Control* (RBAC) asseguram que o utilizador e o dispositivo tem acesso autorizado ao ativo. Tudo isto permite uma maior segurança dos utilizadores e permite responsabilizar o utilizador pelas suas ações.

Pode ser aplicada a utilização de uma rede privada virtual (VPN) remota, que permite o acesso remoto e seguro a rede da empresa do utilizador ou cliente. Cada utilizador tem usualmente do seu lado um *software* de cliente VPN ou baseado em *web browser*. Privacidade e integridade de dados sensíveis é assegurada usando autenticação de multifatores, verificação de conformidade do dispositivo final e encriptação de todos os dados transmitidos.

Para além destes mecanismos existem os modelos de acessos de rede com *zero-trust* e com privilégio mínimo.

Segundo [7], o modelo de privilégio mínimo define que o utilizador apenas deve ter os acessos e permissões mínimas que permitam que este possa desenvolver a sua função. Esta solução permite um acesso granular as aplicações da empresa onde apenas os utilizadores que precisam do acesso para desenvolver o seu trabalho.

O modelo de *zero-trust* é um conjunto de paradigmas de cibersegurança que diverge e afasta de defesas de perímetros estáticos baseados em rede para se focar nos utilizadores, ativos e recursos. Uma arquitetura *zero-trust* usa princípios de *zero-trust* para planear a infraestrutura industrial e empresarial e fluxos de trabalho.

A arquitetura *zero-trust* assume não haver confiança implícita concedida a ativos ou contas de utilizador com base exclusivamente na sua localização física, de rede, ou com base sobre a propriedade de ativos. Autenticação e autorização são funções executadas antes de uma sessão para um recurso da empresa ser estabelecida. A*zero-trust* concentra-se na proteção de recursos, não em segmentos de rede, pois o rede local não é mais vista como o principal componente para a postura de segurança do recurso.

Deve ser aplicada a segurança de endereço eletrónico, sendo esta definida por processos, produtos ou serviços designados para proteger as contas de endereço eletrónico dos utilizadores da empresa de ameaças externas. Apesar de a maioria dos fornecedores de serviços de endereço eletrónico já terem proteções construídas dentro dos seus produtos, estas podem não ser suficientes para a sua proteção, tendo que haver formação dos utilizadores enquanto as ameaças mais comuns.

Deve haver prevenção de perda de dados, sendo uma metodologia que combina tecnologia com as melhores pratica para prevenir a exposição de dados sensíveis para fora da empresa.

Pode ser aplicada a tecnologia *Intrusion Prevention System* (IPS), que permite detetar ou prevenir ataques de segurança da rede e a exploração de vulnerabilidades existentes. A exploração dessas vulnerabilidades, por exemplo, de um *software* ou de um dispositivo, pode levar o atacante a ter controlo da rede e do sistema. Esta tecnologia permite bloquear ataques que ainda não são conhecidos devido à aprendizagem de máquina que aprende como a rede se comporta normalmente e bloqueia comportamentos fora da norma.

Temos ainda o *Sandboxing*, prática que permite correr código ou abrir ficheiros maliciosos num ambiente seguro e isolado numa máquina que simula um sistema operativo de um utilizador. Isto permite observar ficheiros ou código quando é aberto e procurar por comportamento malicioso, prevenindo que se infiltre na rede.

Se possível deve ser aplicada a segurança de rede hiperescalada, permitindo que uma arquitetura de rede escalar seja proporcional como a exigência adicionada no sistema. Isto permite que seja efetuada uma rápida implementação e aumentar ou diminuir a rede para completar as exigências da segurança de rede. Ao integrar recursos de rede e de computação num sistema definido por *software*, é possível utilizar completamente todos os recursos de *hardware* disponíveis.

Relativamente à segurança de rede da nuvem, as aplicações e recursos de computação já não são exclusivamente hospedados num centro de dados local da empresa. Para proteger os centros de dados modernos é preciso uma maior flexibilidade para manter a segurança de dados migrados para a *cloud*. As soluções definidas por meio de *software*, como *Software as a service*, permitem que essas soluções de segurança de rede sejam aplicadas em diversos cenários.

Para finalizar, um Indicador de Compromisso - *Indicator of Compromise* (IOC) é um conjunto de dados relativos a um objeto ou atividade que indica acesso não autorizado a um dispositivo. Por exemplo, muitas tentativas falhadas de iniciar sessão no sistema podem constituir um IOC. A tarefa de verificação de IOCs permite localizar IOCs num dispositivo e adotar medidas de resposta a ameaças.

2.1.3 *Segurança de informação*

A segurança de informação prevê proteger os dados da empresa, mantendo a sua integridade e privacidade, independentemente do seu estado de armazenamento.

A criptografia é a maneira mais eficaz de proteger os dados contra acesso não autorizado. Esta pode ser definida como a transformação dos dados num formato alternativo que só pode ser lido por uma pessoa com acesso a uma chave para decifrar.

Para cifrar dados armazenados em máquinas ou dispositivos existem vários *softwares* disponíveis para esse objetivo. Para a transmissão de dados, deverá ser utilizado um canal de comunicação cifrado. Para transmissão baseada na *web*, deve ser certificado sempre que o *site* utiliza o protocolo SSL.

2.1.4 *Segurança aplicacional*

Segundo [8], a segurança aplicacional prevê a proteção de todas as aplicações usadas pela empresa, usando *software* e atualizações. Também se pode definir pelo processo

de desenvolver, adicionar e testar recursos de segurança nas aplicações para prevenir a exploração de vulnerabilidades e acessos não autorizados. Devido à maioria das aplicações poderem ser acedidas por meio de redes ou da nuvem, este facto aumenta a área de ataque que elas estão expostas e mais rapidamente podem ser encontradas vulnerabilidades, podendo comprometer as mesmas. Existem vários métodos de proteção aplicacionais que podem estar incluídos nas aplicações ou ser feitas por outras aplicações por integrações. Serão expostos alguns métodos para assegurar a segurança aplicacional.

Deverá haver autenticação, sendo um método aplicado no desenvolvimento da aplicação que garante que o utilizador é quem diz ser. Isto permite que haja um não repudio nas ações do utilizador na utilização da aplicação e garante a sua autenticidade. Para garantir a autenticação, normalmente o utilizador tem que fornecer o seu nome de utilizador e *password*, e para segurança adicional a autenticação por multifatores que pode requerer uma *password* adicional, código SMS, código mediante endereço eletrónico, impressão digital ou uma aplicação externa de autenticação.

Após a autenticação, o utilizador deve ter autorização para o acesso e uso da aplicação. O sistema verifica se o utilizador tem autorização para aceder à aplicação verificando uma lista de utilizadores autorizados. O utilizador pode ter só certas autorizações na aplicação e uma lista de autorizações de cada utilizador também deve ser usada. A autorização deve ser feita sempre depois da autenticação para que só sejam validadas contas que estejam na lista autorizada.

A encriptação pode ser usada para garantir a proteção de dados sensíveis, enquanto estes estão guardados no dispositivo ou quando estas estejam em trânsito, sendo que em aplicações alojadas na nuvem devem encriptar sempre o seu tráfego.

Logging permite guardar todos os movimentos realizados numa aplicação, desde dos movimentos do utilizador até aos dados que este acedeu. Se a aplicação permitir *logging* e caso haja uma falha de segurança, será mais fácil identificar o responsável, quais os dados que foram acedidos e o ponto de entrada do atacante.

Os testes de segurança da aplicação são um procedimento necessário para garantir que todos os controlos de segurança funcionam corretamente. Estes testes são realizados no desenvolvimento da aplicação para garantir que não há vulnerabilidades na aplicação que possam ser exploradas. Estes testes devem ser realizados quando o lançamento de novas atualizações da aplicação.

Devem ser aplicados controlos de segurança, para que quando ocorre algo que aplicação não está a espera, como dados que esta não está a espera ou a aplicação é

desligada inesperadamente, os programadores tenham mais controlo sobre o resultado dessas ações. Estas ações, se não forem endereçadas, podem causar vulnerabilidades no sistema que podem ser exploradas.

Deve haver uma auditoria para a aplicação estar nos padrões estabelecidos de segurança. Após a auditoria, os desenvolvedores devem garantir que apenas utilizadores autorizados a podem aceder. Pode ser feito um teste de penetração para encontrar vulnerabilidades que possam ter escapado ou para formar os utilizadores na melhoria da segurança de como usam a aplicação.

2.1.5 *Segurança operacional*

Segundo [9], a segurança operacional prevê a inclusão de processo e decisões de tratamento de dados, decidindo aonde estes são armazenados e quem tem acesso a estes, tendo assim uma hierarquia de permissões. A segurança operacional pode ser categorizada nos seguintes vários passos.

Devem se identificar os dados sensíveis, esses serão os dados mais sensíveis da empresa e o maior foco de proteção deverão ser identificados. Estes incluem informações privadas de clientes, dados financeiros, médicos e dos colaboradores da empresa.

Em cada categoria de informação considerada sensível, devem ser identificadas as suas ameaças. Essas ameaças podem incluir ameaças exteriores que queiram roubar essa informação ou interiores como funcionários insatisfeitos e à falta de formação destes que leva à negligência.

Devem-se verificar medidas já tomadas para assegurar a segurança e verificar se existem falhas nas mesmas ou vulnerabilidades que possa ser exploradas para ganhar acesso aos dados.

Deve ser feita uma classificação das vulnerabilidades detetadas, pela probabilidade de serem exploradas, o dano caso sejam exploradas e o trabalho e tempo necessário para a recuperação dos seus danos. Quanto maior e mais danos causar, maior a prioridade para mitigar os riscos dessa vulnerabilidade.

Deve haver a criação e implementação de planos para eliminar ou mitigar os riscos. Estas medidas devem ser simples e fáceis, para poderem ser implementadas o mais rápido possível para diminuírem os danos causados pela exploração da vulnerabilidade.

2.1.6 *Plano de recuperação de desastre e continuidade de negócio*

Segundo [10], um plano de recuperação de desastre e continuidade de negócio prevê a seja definido um plano para resposta a incidentes informáticos na empresa para que esta possa restaurar operações o mais rápido possível após a ocorrência do mesmo. Dever ser implementado um plano de formação dos colaboradores para que estes aprendam as boas práticas de segurança relativamente à empresa, os seus dados pessoais e aos recursos da empresa.

Para além destes pontos referidos anteriormente há segurança adicional que deve ser aplicada especificamente a este sector.

Segurança física prevê a proteção das instalações critica da empresa como subestações, centrais elétricas e vários locais de produção de energia. Esta proteção física, tanto usando um controlo de permissões do perímetro como proteções físicas que impedem o acesso às instalações, permite que as operações não sejam afetadas por fatores externos.

2.1.7 *Gestão de Informações e Eventos de Segurança*

Segundo [11], a Gestão de Informações e Eventos de Segurança - *Security Information and Event Management* (SIEM) é uma solução que ajuda as organizações a detetar, analisar e responder a ameaças de segurança antes que estas afetem as suas operações. A tecnologia de SIEM recolhe dados de registo de eventos a partir de um conjunto de origens, como *logs* de vários dispositivos ou fluxos de rede, identifica a atividade fora da norma com análise em tempo real e toma as medidas adequadas.

Com estas funcionalidades permite fornecer às organizações visibilidade sobre a atividade nas respetivas redes para poderem responder rapidamente a potenciais ciberataques e cumprir os requisitos de conformidade. Recentemente a tecnologia de SIEM evoluiu para tornar a deteção de ameaças e a resposta a incidentes mais rápida e inteligente com a inteligência artificial, permitindo desta forma uma resposta mais rápida do que um ser humano poderia ter.

As ferramentas de SIEM recolhem, agregam e analisam volumes de dados das aplicações, dos dispositivos, servidores e utilizadores de uma empresa em tempo real para que as equipas de segurança possam detetar e bloquear ataques. As ferramentas de SIEM utilizam regras predeterminadas para auxiliar as equipas de segurança a

definir ameaças e gerar alertas. Estas também permitem regras customizáveis que podem ser feitas à medida das necessidades e enquadramento da empresa.

2.1.8 Software *de deteção de anomalias*

Software de deteção de anomalias é a identificação de itens, eventos ou observações que não estão conforme um padrão esperado. Técnicas de deteção de anomalias não supervisionadas detetam anomalias num conjunto de dados de teste não rotulado sob a suposição de que a maioria das instâncias no conjunto de dados são normais.

Técnicas de deteção de anomalias supervisionadas requerem um conjunto de dados rotulados como normal e anormal e envolve o treino de um classificador. a ser gerado pelo modelo aprendido. O *software* de deteção de anomalias permite que as empresas detetem anomalias identificando padrões incomuns, comportamentos inesperados ou tráfego de rede incomum. O *software* pode comparar itens, eventos ou padrões para medir desvios da base normal. Ele pode detetar anomalias num conjunto de dados categorizado como normal.

O *software* também pode detetar anomalias num conjunto de dados não rotulados e usar um modelo que representa padrões ou comportamentos normais para localizar atividades incomuns. O modelo é baseado numa linha de base comum com inúmeras entradas do que é considerado normal. O *software* de deteção de anomalias usa diferentes técnicas, incluindo métodos estatísticos simples, técnicas baseadas em densidade e técnicas baseadas em *cluster*.

O *software* inclui recursos que permitem aos utilizadores empresariais identificar anomalias únicas, anomalias coletivas e anomalias contextuais. Ele ajuda os utilizadores a localizar comportamentos estranhos que podem indicar um ataque, monitorizar a integridade dos sistemas de negócios e detetar atividades fraudulentas em transações comerciais.

2.1.9 Smart Grids

Segundo a Endesa [12] o uso de *smart grids* serve para a estabilização e otimização da rede energética, podendo ser usada também para a sua monitorização e controlo da mesma. As *smart grids* asseguram também a gestão dos equipamentos e instalações ligadas às mesmas, como a manutenção da rede elétrica.

As *smart grids* funcionam utilizando sensores que avaliam continuamente o funcionamento da rede elétrica equilibrando as cargas. Estes sensores permitem disponibilizar informação sobre os consumos de energia a consumidores e fornecedores para poderem ser feitos os ajustes necessários.

Este conjunto permite que haja uma maior segurança das instalações elétricas como da cibersegurança, pois mesmo que um atacante se infiltre no sistema para destabilizar a rede, a *smart grid* iria sempre estabilizar a mesma.

2.1.10 *Sistemas SCADA*

Segundo [13] o uso de sistemas de monitorização, como o SCADA, permitem colecionar medições e dados dos estados dos sistemas de energia, sendo que um sistema de gestão de energia pode usar estes dados para aumentar a segurança e prevenir a destabilização da rede elétrica.

Os sistemas SCADA permitem:

- Controlo de processos local ou remotamente;
- Adquirir, analisar e mostrar dados num curto espaço de tempo;
- Interagir diretamente com os equipamentos como sensores entre outros;
- Gravar e guardar eventos para referência futura ou criação de relatórios;

Estes sistemas fornecem informações constantes e não síncronas do sistema de energia com o tempo resolução entre 1 e 10 segundos, limitados a medições de estado estacionário e não podem ser usadas para observar a dinâmica do sistema.

2.1.11 Wide Area Monitoring System

Segundo [14], WAMS é uma tecnologia de alerta antecipado que ajuda a prevenir sobrecargas e instabilidades do sistema e disparos em cascata que podem levar a apagões de energia. O *Wide Area Monitoring System* (WAMS) consiste numa série de unidades de medição fasorial que monitorizam cargas e temperaturas nas linhas de energia e permitem que os operadores identifiquem problemas antecipadamente e evitem interrupções generalizadas na rede.

Uma arquitetura WAMS é composta por PMUs, PDCs, redes de comunicação, armazenamento de dados e *software* aplicativo. Requisitos do sistema de energia

determinam o número de PDCs da subestação. As PMUs instaladas nas subestações medem tensão, corrente e frequência. Essas medições são enviadas diretamente para o PDC central ou para um PDC da subestação.

O PDC da subestação possui as seguintes funcionalidades:

- adquire dados de PMUs
- sincronização de tempo de dados
- avalia os dados recebidos
- envia dados para o PDC central
- troca de dados com o SCADA local
- arquiva dados localmente
- realiza análises de dados locais e ações de proteção.

O uso de um PDC da subestação é recomendado em caso de má comunicação entre a subestação e o sistema central. Em tais situações, o PDC da subestação serve como registador de dados local em caso de interrupção da comunicação. Contudo, se muitas PMUs estiverem instaladas na subestação, ela envia apenas dados selecionados para o PDC central. No caso de sistemas de energia maiores, um PDC regional pode ser aplicado entre as subestações e o PDC central.

Um PDC central adquire dados dos PDCs e PMUs da subestação e sincroniza dados pela etiqueta de tempo e executa a avaliação de dados. Os dados sincronizados são usados para diferentes aplicativos WAMS, troca de dados com outros sistemas como SCADA/ EMS ou troca de dados entre empresas. Adicionalmente, os dados são usados na visualização em tempo real e arquivamento de dados.

A comunicação entre PMUs, PDC da subestação e PDC central usam IP nas comunicações de rede. Com base nesse padrão, os dados do sincrofasor podem ser transportados por qualquer sistema de comunicação que tenha largura de banda suficiente. A largura de banda necessária é dedicada pela taxa de relatórios e pelo tamanho da mensagem.

2.2 BARREIRAS ATUAIS PARA O MELHORAMENTO DA SEGURANÇA NO SECTOR ELÉTRICO

Segundo [15], existem enumeras barreiras que retêm o sector energético de se conseguir proteger adequadamente de ciberataques. Sendo que não há segurança

infalível, estas barreiras ao serem superadas iriam levar a um maior investimento na área de segurança, uma maior comunicação entre entidades relativamente a ameaças e por conseguinte a uma maior segurança.

As principais barreiras para o melhoramento são:

- As ameaças cibernéticas são imprevisíveis e evoluem mais rapidamente do que a capacidade do setor de se desenvolver e implantar contramedidas;
- As atualizações de segurança para sistemas antigos são restringidas por limitações relacionadas com os equipamentos e arquiteturas;
- O teste de desempenho/aceitação de novas soluções de controlo e comunicação é difícil sem interromper as operações;
- A partilha de informações sobre ameaças, vulnerabilidades, incidentes e mitigação é insuficiente entre o governo e a indústria;
- Muitos negócios vêm a área de cibersegurança como fraco investimento pela indústria;

Isto determina que o sector possui vários obstáculos a ultrapassar para melhorar a sua segurança.

2.3 TECNOLOGIA OPERACIONAL

Segundo [16], os dispositivos OT são geralmente controlados por DCS ou por PLCs. Antigamente, a maioria dos dispositivos OT foram protegidos por *air-gapping* — isolamento físico do dispositivo de redes externas. Devido ao ambiente industrial estar a experimentar uma convergência de IT e OT, significa a existência de novos riscos e o *air-gapping* não é eficaz. Para isto serão referidas algumas tecnologias operacionais usadas tanto no sector energético como no sector industrial.

Uma das tecnologias usadas é o controlador lógico programável (PLC), sendo este um tipo de computador minúsculo que pode receber dados por meio de entradas e enviar instruções de operação por meio de saídas. O trabalho de um PLC é controlar as funções de um sistema usando a lógica interna programada nele, automatizando assim os processos usados pela empresa.

Um PLC recebe entradas, seja de pontos de captura de dados automatizados ou de pontos de entrada humana, como interruptores ou botões. Com base na sua programação, o PLC decide então se deve ou não alterar a saída. As saídas de um PLC podem controlar uma grande variedade de equipamentos, incluindo motores,

luzes ou interruptores. Normalmente os PLCs estão localizados nas proximidades dos sistemas em que operam e são normalmente protegidos por uma caixa elétrica.

São usadas também unidades de terminais remotas (RTU), sendo estes dispositivos de controlo normalmente instalados num local remoto como parte de um grande sistema. O principal objetivo de uma RTU é monitorizar e controlar dispositivos de campo, como válvulas, atuadores, sensores, entre outros. As RTUs são componentes essenciais dos sistemas de SCADA, estabelecendo *interfaces* entre o controlo SCADA e os processos físicos.

Outra tecnologia usada é a unidade de medição fasorial (PMU), sendo esta uma ferramenta chave usada em sistemas elétricos para melhorar a visibilidade dos operadores sobre o que acontece em toda a rede elétrica. Uma PMU é um dispositivo que mede uma grandeza chamada fasor sendo que este informa a magnitude e o ângulo de fase da tensão num local específico numa linha de energia. Essas informações também podem ser usadas para determinar a frequência e são úteis para identificar e analisar as condições do sistema. As PMUs fornecem até 60 medições por segundo, o que é muito mais do que uma medição típica a cada 2 a 4 segundos fornecida pelos sistemas SCADA convencionais. As PMUs têm uma grande vantagem sobre os meios tradicionais de medição de dados porque todos os dados da PMU são marcados com o uso de dados GPS. Isso significa que os dados coletados numa grade são todos sincronizados usando o mesmo método exato de associar o tempo aos dados.

São usados também sistemas de controlo industrial (ICS), sendo estes diferentes tipos de sistemas de controlo e instrumentação associada, que incluem os dispositivos, sistemas, redes e controlos usados para operar e/ou automatizar processos industriais. Dependendo do setor, cada ICS funciona de maneira diferente, sendo construído para gerir tarefas eletronicamente com eficiência.

O sistema de controlo distribuído (DCS) usado também nas indústrias, sendo um sistema para controlar os sistemas de produção encontrados num local. Num DCS, um ponto de ajuste é enviado ao controlador que consegue instruir as válvulas, ou um atuador, a operar para que o ponto de ajuste desejado seja mantido. Os dados do campo podem ser armazenados para referência futura, usados para controlo de processos simples ou até mesmo para estratégias avançadas de controlo com dados de outra parte da planta.

Cada DCS usa um *loop* de controlo de supervisão centralizado para gerir vários controladores ou dispositivos locais que fazem parte do processo geral de produção. Isso dá às indústrias a capacidade de ver rapidamente os dados de produção e opera-

ção. Usando vários dispositivos no processo de produção, um DCS consegue reduzir o impacto de uma única falha no sistema geral. Um DCS também é normalmente usado em indústrias como fabricação, geração de energia elétrica, fabricação de produtos químicos, refinarias de petróleo e tratamento de água e águas residuais.

Um dos componentes que serve para monitorizar é a Interface Homem-Máquina - *Human Machine Interface* (HMI), sendo um aplicativo de Interface Gráfica de Utilizador - *Graphical User Interface* (GUI) que permite a interação entre o operador humano e o *hardware* do controlador. Ele também pode exibir informações de estados e dados históricos recolhidos pelos dispositivos no ambiente ICS. Também é usado para monitorizar e configurar pontos de ajuste, algoritmos de controlo e ajustar e estabelecer parâmetros nos controladores.

Um dos componentes críticos são os *Phasor Data Concentrator* (PDC), sendo dispositivos que agregam e sincronizam dados fasoriais transmitidos de PMUs de toda a rede. Um PDC é uma ligação crítica entre as PMUs que recolhe os dados fasoriais e as aplicações de sincrofasores que usam os dados, como, por exemplo, os sistemas SCADA. As capacidades destes dispositivos as seguintes: o registo de dados agregados, encaminhamento de dados, validação de dados, apoio ao protocolo de transferência de dados, conversão de protocolos de transferência de dados, conversão de coordenadas e cálculo da latência de dados. Estes dispositivos permitem que haja troca e processamento de dados em tempo real entre outras aplicações, armazenamento de dados e visualização destes.

Para monitorização mais alargada da rede é usado um sistema de controlo, supervisão e aquisição de dados (SCADA). Este não é um sistema que pode fornecer controlo total. Em vez disso, a suas capacidades estão focadas em fornecer controlo no nível de monitorização. Os sistemas SCADA são compostos por dispositivos, geralmente PLCs ou RTUs distribuídos em vários locais. Os sistemas SCADA podem adquirir e transmitir dados sendo integrados a uma HMI que fornece monitorização e controlo centralizados para várias entradas e saídas de processo.

O objetivo principal do uso do SCADA é a monitorização e controlo de longa distância de locais de campo por meio de um sistema de controlo centralizado. Isto permite que um sistema SCADA consiga automatizar essas tarefa manuais realizadas anteriormente. Os dispositivos de campo controlam as operações locais, como abertura ou fechamento de válvulas e disjuntores, recolha de dados dos sistemas de sensores e monitorização do ambiente local.

Os sistemas SCADA são normalmente usados em indústrias que envolvem monitorização e controlo de ductos, centros de tratamento e distribuição de água e transmissão e distribuição de energia elétrica.

Com estas tecnologias e o paradigma atual que leva à convergência das redes OT e IT, levando a que estes normalmente ocupem esferas separadas de preocupação na indústria de energia e serviços públicos. IT tende a ter estratégias e políticas globais enquanto OT sempre foi localizado. O *software* é adquirido localmente e os fluxos de trabalho, processos e procedimentos foram todos desenvolvidos localmente.

Para diagnosticar, manter, monitorizar e otimizar os equipamentos industriais físicos que impulsionam os negócios são usados os dispositivos IoT, como sensores, sendo estes integrados em plantas de energia, tubos de transporte ou turbinas eólicas. O objetivo destes não é apenas que a IT entenda e gire melhor os dados que a OT lida diariamente, mas produzindo-os e usando-os, reduzindo redundâncias e erros e melhorar os fluxos de trabalho e a eficiência.

Por exemplo, dispositivos inteligentes podem monitorizar equipamentos em busca de sinais de mau funcionamento e, em seguida, acionar uma visita do engenheiro de serviço. Com a inteligência artificial, esses dispositivos também podem analisar dados suficientes para começar a identificar áreas onde os sistemas OT possam ser melhorados ou como uma rede elétrica pode ser melhor equilibrada.

2.4 GESTÃO, MONITORIZAÇÃO, PROTEÇÃO E CONTROLO DA REDE ELÉTRICA

Segundo [15], os dispositivos e redes de OT para sistemas de fornecimento de energia permitem que os operadores mantenham a consciência situacional, enviem economicamente recursos energéticos, planeiem contingências e equilibrem a geração com a carga em tempo real. Esses recursos são geralmente fornecidos por um Sistema de Gestão de Energia - *Energy Management System* (EMS) que reside num centro de controlo de utilidade e realiza estimativas de estado, análise de contingência e Controlo Automático de Geração - *Automatic Generation Control* (AGC). O EMS recebe dados de um sistema SCADA que adquire medições de operação do sistema de energia a cada dois a cinco segundos de dispositivos especializados em subestações.

O estimador de estado EMS usa dados SCADA, dados transmitidos por meio do *Intercontrol Center Communication Protocol* (ICCP) de outros centros de controlo

de concessionárias e as leis da física para estimar o estado operacional da rede elétrica a cada poucos minutos. Essas informações fornecem aos operadores a consciência situacional para tomar decisões informadas, como fluxo de energia otimizado para despacho de geração económica e eficiente. Os estimadores de estado também detetam e rejeitam dados corrompidos de sensores com defeito. Novos métodos, como o *Security-Oriented Cyber-Physical State Estimation* (SCPSE), foram desenvolvidos para detetar dados que foram comprometidos de forma maliciosa com a intenção de deturpar as operações da rede.

O EMS realiza análise de contingência em tempo real para antecipar instabilidades da rede que podem resultar de uma falha importante de um componente da rede, como a perda de um gerador ou linha de transmissão.

Esta análise mostra como as condições de operação da rede elétrica podem evoluir em resposta à perda de componentes específicos naquele momento e apoia o planeamento para garantir que os limites operacionais da rede não sejam violados se tal instabilidade ocorrer. Esquemas de ação corretiva automatizada ou sistemas de proteção especial garantem que a rede permaneça estável mesmo se um componente importante for perdido inesperadamente. Do ponto de vista da segurança cibernética, as consequências físicas de comandos maliciosos podem ser modeladas como contingências para avaliar o risco e desenvolver mitigações com bastante antecedência.

O AGC permite que uma autoridade de balanceamento ajuste a geração para atender à procura de energia em tempo real conforme a carga se conecta e se desconecta da rede. Dispositivos de proteção e controlo, como dispositivos eletrónicos inteligentes (IEDs) com sistemas operativos embarcados, são usados na geração, transmissão e, cada vez mais, nos níveis de distribuição. Esses dispositivos medem e reagem automaticamente às condições de operação da rede em milissegundos, alguns ciclos a 60 Hz, para evitar que o equipamento exceda os limites operacionais seguros e mantenha a rede estável.

2.5 O QUE SÃO NORMAS DE CIBERSEGURANÇA E QUAIS EXISTEM

Uma norma é o *standard* de comportamento apropriado dos atores de uma determinada entidade. No caso da cibersegurança será o *standard* usado internacionalmente pelas várias instituições relativamente à cibersegurança e como a manter. Estas normas podem ser meramente indicativas e apenas servem de referência, apesar de ser expectável o cumprimento das mesmas, ou obrigatórias, juridicamente vinculadas

e têm que ser cumpridas.

Segundo o Grupo de Especialistas Governamentais das Nações Unidas [17], e a sua definição de normas de cibersegurança, relatório emitido em 2015, estas normas não procuram limitar nem proibir a ação consistente com a lei internacional. As normas refletem as expetativas da comunidade internacional, adicionam *standards* para o comportamento de Estados e permitem que a comunidade internacional avalie as atividades e intenções dos Estados. Para este fim foram criadas normas para atingir o objetivo explicado anteriormente. Estas são:

- Estados não devem atacar companhias de tecnologia de comunicação e informação para inserir vulnerabilidades ou tomar ações que poderão diminuir ou afetar a confiança pública dos produtos e serviços;
- Estados devem ter uma política clara baseada em princípios para lidar com vulnerabilidades de produtos e serviços, sendo que devem denunciá-las aos seus fornecedores e não explorá-las;
- Estados devem exercer restrição no desenvolvimento de armas cibernéticas e devem garantir que as que são desenvolvidas são limitadas, precisas e não reutilizáveis:
- Estados devem se comprometer a não proliferação de armas cibernéticas;
- Estados devem limitar o seu relacionamento relativamente a operações ofensivas cibernéticas para evitar a criação de eventos massivos;
- Estados devem assistir o sector privado na deteção, contenção, resposta e recuperação a eventos cibernéticos;
- Os Estados devem cooperar no desenvolvimento e na aplicação de medidas para aumentar a estabilidade e a segurança no uso das Tecnologias de Informação e Comunicação (TIC) e prevenir práticas de TIC consideradas prejudiciais ou que possam representar uma ameaça à paz e à segurança internacional;
- No caso de incidentes de TIC, os Estados devem considerar todas as informações relevantes, incluindo o contexto mais amplo do evento, desafios de atribuição e a natureza e extensão das consequências provocadas pelo incidente;
- Os Estados não devem permitir conscientemente que o seu território seja usado para atos internacionalmente ilícitos usando TIC's;

- Os Estados devem considerar a melhor forma de cooperar para trocar informações, ajudar reciprocamente, condenar o uso terrorista e criminoso das TIC e implementar outras medidas de cooperação para lidar com essas ameaças;
- O Estado deve garantir o pleno respeito pelos direitos humanos, incluindo o direito à liberdade de expressão;
- Um Estado não deve conduzir ou apoiar conscientemente atividades de TIC contrárias às suas obrigações sob o direito internacional que prejudiquem intencionalmente a infraestrutura crítica ou que de outra forma prejudiquem o uso e a operação da infraestrutura crítica para fornecer serviços ao público;
- Os Estados devem proceder à proteção de infraestruturas críticas contra ameaças de TIC, considerando a Resolução 58/199 (2003) da AGNU "Criação de uma cultura global de segurança cibernética e proteção de infraestrutura de informação crítica";
- Os Estados devem responder às solicitações apropriadas de assistência de outro Estado cuja infraestrutura crítica esteja sujeita a atos maliciosos de TIC. Os Estados também devem responder às solicitações apropriadas para mitigar atividades maliciosas de TIC voltadas para a infraestrutura crítica de outro Estado que emana do seu território, considerando a soberania.
- Garantir a integridade da cadeia de abastecimento.
- Os Estados devem procurar prevenir a proliferação de ferramentas e técnicas de TIC maliciosas e o uso de funções ocultas nocivas
- Incentivar o relato responsável de vulnerabilidades de TIC e a partilha de informações associadas
- Os Estados não devem conduzir ou apoiar conscientemente atividades que prejudiquem os sistemas de informação das equipas autorizadas de resposta a emergências de outro Estado.
- Um Estado não deve usar equipas autorizadas de resposta a emergências para se envolver em atividades internacionais maliciosas.

Estas normas foram aprovadas pelo *The Hague Program for Cyber Norms* [18]. Este programa concentra-se no desenvolvimento e implementação de normas cibernéticas que possam ser aplicadas internacionalmente.

2.6 O QUE É O SECTOR ENERGÉTICO E QUAIS AS SUAS ENTIDADES REGULADORAS

O sector energético e a indústria associada envolve a produção e venda de energia, incluindo a extração de combustível, produção, refinamento e distribuição deste. Este sector é composto por várias indústrias sendo estas:

- Indústria de combustíveis fósseis;
- Indústria de energia elétrica;
- Indústria de energia nuclear;
- Indústria de energia renovável;
- Indústria de energia tradicional;

A indústria de combustíveis fosseis foca se nas indústrias de petróleo (refinação, transporte e venda), na indústria de carvão (extração e processamento) e industria de gás natural(extração, distribuição e venda).

A indústria de energia elétrica foca se na geração de energia elétrica, na sua distribuição e venda, usando o material refinado pela indústria de combustíveis fosseis.

A indústria de energia nuclear foca se no uso de reatores nucleares para produção de energia elétrica, sendo usado materiais como o urânio e o plutónio. Esta industria faz o processamento das matérias-primas usadas, produção da energia e disposição do material emitido por esta.

A indústria de energia renovável foca-se no uso de energias alternativas e sustentáveis como a hidroelétrica, solar e eólica, realizando a sua produção, distribuição e venda.

A indústria de energia tradicional foca-se no uso, corte, coleção e distribuição de madeira para aquecimento e para cozinhar alimentos.

Relativamente ao sector energético em Portugal, todos os consumidores podem escolher o seu fornecedor energético, e todas as corporações que integram o Sistema Elétrico Nacional devem disponibilizar energia elétrica adequada relativamente às necessidades dos consumidores e ser o mais eficiente possível nos meios a utilizar. Estas corporações tem as obrigações de garantir a segurança, a regularidade e a qualidade do seu abastecimento, garantir a universalidade de prestação do serviço, garantir a ligação de todos os clientes às redes e garantir a proteção dos consumidores em relação a tarifas e preços.

A entidade reguladora em Portugal do sector energético é a Entidade Reguladora do Sector Energético (ERSE)[1], regulando todas as indústrias envolvidas no sector a nível nacional como a gestão das suas operações. Esta entidade é governada por uma estrutura de leis de autoridades regulatórias, legislações especifica ao sector e regras e procedimentos relativas ao mesmo. Esta entidade não está afiliada ao governo nacional, sendo uma entidade independente em termo organizacional, funcional e técnico.

A nível europeu operam duas entidades relacionadas com a regulação do sector energético:

- Agency for the Cooperation of Energy Regulators (ACER) [2]
- Council of European Energy Regulators (CEER) [3]

ACER é uma agência estabelecida pela União Europeia para assistir o trabalho das agências regulatórias nacionais dos estados-membros e incentivar coordenação e cooperação mutua a nível europeu. Mais especificamente, permite complementar e coordenar o trabalho das agências regulatórias nacionais, ajudar a formular as regras da rede europeia, publica opiniões, recomendações ou decisões vinculativas em termos e condições de acesso e operações de segurança em infraestrutura transfronteiriça, monitoriza os mercados energéticos europeus e a sua transparência e integridade sobre a *EU Regulation 1227/2011 on wholesale energy market integrity 'I&' transparency*"[4].

CEER é uma agência sem fins lucrativos belga que reúne agências regulatórias de 39 países europeus que tem como objetivos desenvolver o mercado energético a nível europeu para beneficiar o consumidor energético, serve como fórum para troca de conhecimento e experiência entre reguladores, promover soluções para problemas comuns que todos os países envolvidos possuem e promover e defender o ponto de ver que os reguladores possuem com as empresas do sector. O objetivo geral da CEER é facilitar a criação de um mercado europeu interno único, competitivo, eficiente e sustentável para eletricidade.

Para o regulamento da cibersegurança europeia existe a agência da união europeia para a cibersegurança. Esta agência é dedicada a alcançar um alto nível comum de cibersegurança em toda a Europa. Foi estabelecida em 2004 e fortalecida pela Lei de Cibersegurança da UE, contribui para a política cibernética da União Europeia,

1 https://www.erse.pt/en/institutional/erse/about-erse/
2 https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/agency-cooperation-energy-regulators-acer_en
3 https://icer-regulators.net/icer-members/council-of-european-energy-regulators/
4 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011R1227

aumenta a confiabilidade dos produtos, serviços e processos de TIC com esquemas de certificação de cibersegurança, coopera com os Estados Membros e órgãos da União Europeia. Para este objetivo foi criado a diretiva NIS, uma legislação de segurança cibernética em toda a União Europeia que harmoniza as capacidades nacionais de segurança cibernética, a colaboração transfronteiriça e a supervisão de setores críticos em toda a União Europeia, incluindo o sector energético.

2.7 STANDARDS

2.7.1 *ISO 9001*

Segundo a *Société Générale de Surveillance* (SGS) [19], esta norma posiciona-se como parte integrante dos esforços da empresa em direção ao objetivo mais amplo do desenvolvimento sustentável e promove-a como uma ferramenta para melhorar o desempenho global da empresa. Incentiva um maior foque nas partes interessadas internas e externas como parte da adoção de uma abordagem à gestão da qualidade baseada no risco, e enfatiza a importância de adotar um Sistema de gestão de qualidade como uma decisão estratégica para a empresa.

Alguns dos requisitos mais importantes da norma são:

- O contexto de uma empresa refere-se à combinação de fatores e condições internos e externos que podem ter um efeito na abordagem que uma empresa tem dos seus produtos e/ou serviços;
- Uma empresa deve considerar quer o seu contexto, quer as suas partes interessadas ao planear e implementar o seu sistema de gestão de qualidade;
- Uma parte essencial do sistema de gestão de qualidade é identificar os riscos e as oportunidades que tenham um potencial impacto sobre o funcionamento e o desempenho do seu sistema de gestão de qualidade. Após identificar estas questões, externas e internas, relevantes para o seu contexto, bem como as necessidades das partes interessadas, é necessário que uma empresa use essas informações para determinar os riscos e as oportunidades a elas associadas, bem como ações proporcionadas para as tratar;
- A administração é obrigada a demonstrar um maior envolvimento direto no Sistema de gestão de qualidade da empresa e a ausência da necessidade de haver um Representante da Gestão específico é, em parte, uma tentativa

de garantir que o sistema de gestão de uma empresa não é simplesmente propriedade de um único indivíduo. Há agora uma ênfase na liderança em vez de apenas na gestão do sistema de gestão de qualidade;

- Identificação das competências necessárias para os colaboradores cuja função afeta o desempenho de qualidade;
- Identificação e manutenção do conhecimento necessário para assegurar que uma empresa pode alcançar a conformidade de produtos e serviços;

Para as empresas que já têm um sistema de gestão de qualidade não haverá necessidade de alterar a estrutura documental do seu Sistema de gestão de qualidade ou a terminologia que utiliza, para espelhar a que consta nesta norma.

2.7.2 *ISO 14001*

Segundo [20], esta norma prevê requisitos para a gestão mais eficaz dos aspetos ambientais das atividades da empresa, tendo em consideração a proteção ambiental, prevenção da poluição, cumprimento legal e necessidades socioeconómicas.

A norma valoriza a reputação de qualquer empresa, apoiando no cumprimento da legislação ambiental e a reduzir os riscos de sanções e ações judiciais.

A conformidade com a norma assegura à empresa um uso racional de energia e recursos, além da redução dos custos ao longo do tempo. Por este modo, a certificação ajuda a desenvolver e a melhorar o desempenho da empresa.

A conformidade com a norma permite demonstrar elevados níveis de conformidade ambiental nos concursos a contratos internacionais ou na expansão local de novos negócios.

2.7.3 *ISO 50001*

Segundo [21], a gestão eficiente da energia é uma prioridade das empresas, não só pelo potencial significativo de redução de custos, como também pelo seu papel na redução de emissões de gases com efeito de estufa.

Um sistema de gestão de energia baseado nesta norma é parte integrante de um sistema global de gestão de uma empresa, que tem como objetivos estabelecer os sistemas e processos necessários para melhorar o desempenho energético global da empresa, incluindo a utilização, consumo e eficiência energética. Esta norma inter-

nacional é aplicável a todos os tipos e dimensões de empresas, independentemente das suas condições geográficas, culturais e sociais.

Esta norma tem um elevado nível de compatibilidade, permitindo a integração com outros sistemas de gestão existentes.

A norma não estabelece nenhumas exigências de desempenho energético, mas disponibiliza um conjunto de requisitos e metodologias de suporte para as empresas definirem as suas metas, melhorando continuamente o seu desempenho.

Os principais benefícios da implementação desta norma são a promoção da eficiência energética na empresa, a redução dos impactes ambientais, o impulso para utilização de energias alternativas e renováveis, o cumprimento requisitos legais, a redução de custos e o reforço da imagem da empresa relativamente às preocupações climáticas.

2.7.4 *ISO 45001*

Segundo o [22], o grande foco da norma é o contexto empresarial. A norma exige que a empresa tenha em conta a expectativa dos seus *stakeholders* relativamente à gestão da saúde e da segurança ocupacional. A empresa deve determinar quem são as pessoas relevantes para o seu Sistema de Gestão da Saúde e Segurança Ocupacional e estabelecer os requisitos pertinentes para as partes interessadas.

As áreas incluídas no foco desta norma são:

- A administração deve demonstrar o seu envolvimento com o sistema de gestão da saúde e segurança ocupacional com uma participação direta, levando a saúde e a segurança ocupacional em conta no planeamento estratégico;
- A administração deve contribuir para a eficácia do sistema de gestão da saúde e segurança ocupacional atuando ativamente na sua orientação, suporte e comunicação com os colaboradores, promovendo e liderando a cultura organizacional do sistema de gestão da saúde e segurança ocupacional;
- A norma exige que a administração da empresa incentive a consulta e a participação de colaboradores e os seus representantes, ao serem fatores essenciais para a gestão de saúde e a segurança ocupacional;
- A consulta implica uma comunicação transversal e envolve o fornecimento pontual de informações que os colaboradores e os seus representantes necessitam antes que a empresa possa decidir;

- O sistema de gestão de saúde e a segurança ocupacional depende da participação dos colaboradores. Isto permitirá que contribuam no processo de tomada de decisões sobre o desempenho de saúde e a segurança ocupacional e ofereçam opinião sobre as mudanças propostas;
- A empresa deve incentivar os colaboradores de todos os níveis a comunicar situações perigosas para ser possível adotar medidas preventivas e ações corretivas. Os colaboradores também devem conseguir comunicar e sugerir áreas de melhoria sem medo de represálias.
- A norma exige que a empresa assegure que os processos de contratação externa que afetam o seu sistema de gestão da saúde e segurança ocupacional sejam definidos e controlados.
- Quando o fornecimento de produtos e/ou serviços de contratação externa está sob o controlo da empresa, o risco do fornecedor e do contratado deve ser gerido com eficácia.

Estes pontos permitem fornecer à empresa um alto nível de compreensão das questões que podem afetar como esta gere as suas responsabilidades de saúde e segurança ocupacional em relação aos seus colaboradores.

2.7.5 *ISO 27001*

International Organization for Standardization (ISO) é o sistema mundial especializado em estandardização, sendo composta por diversos comités de vários países que queriam participar no desenvolvimento de *standards* uniformes internacionalmente.

O objetivo do ISO 27001:2017 é proporcionar linhas de guia para ser estabelecida, implementada, e melhorada ao longo do tempo um Sistema de Gestão de Segurança de Informação (SGSI). A forma como este pode e deve ser implementado depende sempre do tamanho e objetivos da empresa em que o SGSI irá ser implementado, sendo que estes que podem mudar ao longo do tempo. O sistema deve escalar sempre com as necessidades da empresa.

O SGSI deve fornecer a confidencialidade, integridade e a disponibilidade da informação fazendo uma análise de riscos.

Existem vários requerimentos que a empresa deve cumprir sendo estes:

- A empresa em que o SGSI está inserido é que decidirá os problemas internos e externos que são relevantes para os seus objetivos e que afetam o objetivo do SGSI;
- A empresa determinará que partes envolvidas são relevantes para o SGSI e se esta tem requerimentos relevantes para o SGSI;
- A empresa determinará aonde é aplicável o SGSI para determinar o âmbito do mesmo, sendo que os descritos anteriormente irão permitir a empresa determinar onde pode ser aplicado o SGSI;
- A empresa deve estabelecer, manter e melhorar continuamente o SGSI, de acordo com o ISO 27001;

A administração da empresa deve mostrar liderança e respeito pelo SGSI, sendo que deve garantir que:

- O SGSI foi estabelecido com a direção estratégica da empresa e os objetivos do SGSI;
- O SGSI é integrado nos processos da empresa;
- O SGSI tem os recursos necessários para o seu funcionamento;
- A empresa é informada da importância do SGSI e que esta está em conformidade com os requerimentos do SGSI;
- O SGSI atinga o seu objetivo;
- Direcione e suporte pessoal que contribuam a eficácia do SGSI;
- Promover o seu melhoramento continuo;
- Suporte outros cargos de gestão que provem a sua liderança e que apliquem as suas capacidades;

A gestão de cargos deve estabelecer políticas de segurança que:

- Sejam apropriadas para a empresa
- Incluam ou ajudem a criar uma estrutura para a criação de objetivos de informação
- Incluam um compromisso para cumprir os requerimentos e o continuo melhoramento do SGSI
- Que estejam disponíveis em documentação.
- Que sejam comunicadas dentro da empresa e a todas as partes interessadas.

A gestão de cargos deve assegurar que os cargos relevantes para a SGSI sejam atribuídos e comunicados e deve atribuir a responsabilidade e autoridade para garantir que o SGSI segue os requerimentos do ISO 27001 e que o SGSI comunica a performance à administração da empresa.

Quando a empresa planear o SGSI deve considerar os problemas e requerimentos que esta tem e determinar o que deve ser feito para:

- Que o SGSI atinja o objetivo pretendido;
- Que sejam reduzidos ou anulados os efeitos indesejados e que haja um contínuo melhoramento do SGSI;

A empresa deve planear ações para dar resposta aos riscos e oportunidades, sendo que deve integrar essas ações no SGSI e avaliar a eficácia das mesmas.

A empresa deve definir e aplicar um processo de avaliação de riscos de segurança de informação que estabeleçam e mantenham um critério desses mesmos riscos para que inclua riscos aceitáveis e critérios de avaliação dos riscos segurança informáticos.

A empresa deve assegurar que as avaliações dos riscos de segurança informáticos produzam resultados consistentes, válidos e possam ser comparados.

A empresa deve identificar os riscos de segurança de informação e aplicar o processo de avaliação desses mesmos riscos que estejam associados a perda de confidencialidade, integridade e disponibilidade dentro do alcance do SGSI, identificando a quem pertencem os riscos. A empresa deve analisar os riscos de segurança e analisar se estes podem se realizar, as consequências se estes acontecerem e o nível desses mesmos riscos.

A empresa deve avaliar os riscos de segurança, comparando os resultados dos mesmo em relação aos critérios de risco criados e tratar da análise dos mesmos, sendo que deve ser documentado todos os processos anteriormente descritos.

A empresa deve definir e aplicar processos para tratamento dos riscos de segurança de informação para apurar a melhor opção de tratamento dos riscos tendo em conta a análise dos mesmos, escolhendo todos os controlos necessários para a implementação da opção escolhida e produzir uma confirmação de aplicabilidade que contenha todos os controlos necessários, justificando a sua inclusão e se estes foram implementados na sua totalidade.

A empresa deve formular um plano para tratamento de dados dos riscos de segurança de informação e obter a aprovação da entidade a quem pertencem os riscos dos planos de tratamentos desses riscos.

A empresa deve manter a documentação todo o processo de tratamento dos riscos de segurança informática.

A empresa deve estabelecer objetivos de segurança de informação, sendo que estes devem ser:

- Consistentes com a política de segurança de informação;
- Mensuráveis;
- Levados nem conta a aplicabilidade os requerimentos do sistema de segurança, nos resultados da avaliação dos riscos e do seu tratamento;
- Comunicados e atualizados quando for necessário;

Todos os processos dos objetivos de segurança de informação devem ser documentados pela empresa.

A empresa, ao planear como atingir os objetivos da segurança de informação, deve determinar como serão atingidos, que recursos serão utilizados, quem será responsável, quando serão atingidos e como os resultados destes serão avaliados.

A empresa deve determinar e disponibilizar os recursos necessários para a criação, implementação, manutenção e atualização do SGSI. A empresa deve:

- Determinar se o pessoal envolvido na mesma tem as competências necessárias e se estas afetam a performance do sistema de segurança;
- Assegurar que o pessoal tem as competências necessárias baseadas na educação, experiência e/ou treino;
- Caso necessário, fornecer a necessária experiência, treino ou educação e avaliação se estes são eficazes;

Este processo deve ser documentado e retido como evidência da competência do pessoal.

O pessoal que trabalha para a empresa deve ter conhecimento da política de segurança de informação, da sua eficácia para a performance do SGSI e dos benefícios que tem para o mesmo e as consequências caso não cumpra com os requerimentos do SGSI.

A empresa deve determinar a necessidade para comunicação interna e externa relevante ao SGSI, sendo o que comunicar, a quem comunicar, com quem comunicar, quem irá comunicar e como irá ser feita a comunicação. O SGSI da empresa deve incluir informação da documentação apresentada pela ISO e documentação necessária, determinada pela empresa, para a eficácia da mesma. O tamanho da

documentação relativa ao SGSI depende sempre do tamanho da empresa, da sua área de atividade, complexidade e da competência do pessoal. A empresa, quando cria ou atualiza a documentação, deve assegurar a apropriada identificação, descrição e formato da mesma, sendo esta aprovada e adequada. A documentação requerida pelo SGSI e pela ISO deve ser controlada para garantir que está sempre disponível e utilizável quando precisa e protegida.

A empresa, para controlo da documentação, deve garantir, se aplicável à mesma, como a documentação:

- É distribuída, usada e acedida;
- É guardada e preservada;
- É controlada as atualizações da mesma;
- É feita a retenção e eliminação da mesma;

A documentação externa que seja necessária para o planeamento e gestão do SGSI, determinada pela empresa, deve ser identificada e controlada. A empresa deve planear, implementar e controlar os processos necessários para garantir os requerimentos da segurança de informação e aplicar as ações determinadas anteriormente. A empresa deve implementar planos para completar os objetivos de segurança de informação descritos anteriormente. A empresa deve controlar as mudanças planeadas e rever as consequências dessas caso sejam acidentais e tomar ações para mitigar efeitos adversos.A empresa deve assegurar que processos que são terceirizados, sejam controlados. A empresa deve fazer avaliações periódicas ao risco de segurança de informação em intervalos planeados ou quando forem feitas mudanças significativas. A empresa deve reter documentação de todos os resultados da avaliação de riscos. A empresa deve implementar um plano para tratamento dos riscos de segurança de informação e devem ser documentados os resultados do mesmo tratamento.

Relativamente à avaliação de performance do SGSI,a empresa deve avaliar a performance em relação à segurança de informação e a eficácia do SGSI e determinar o que deve ser monitorizado e avaliado, podendo ser esses processos e/ou controlos de segurança de informação.

A empresa deve avaliar métodos para monitorização, medição, análise e avaliação para garantir que são produzidos resultados válidos. A empresa deve determinar quando é feita a monitorização e medição será feita, por quem, quando os resultados serão analisados e avaliados e quem os irá fazer, sendo este processo documentado para servir de evidência dos resultados de monitorização e medição. A empresa deve

fazer auditorias internas em intervalos para avaliar se o SGSI segue os requerimentos da empresa para o SGSI e para os requerimentos do ISO, verificando se este se encontra eficaz e propriamente mantido.

A empresa deve:

- Planear, estabelecer, implementar e manter um programa de auditorias, que deve incluir a frequência, métodos, responsabilidades, requisitos de planeamento e relatórios;
- Definir critérios para cada auditoria e os tamanhos da mesma;
- Selecionar os auditores e realizar auditorias que assegurem objetividade e imparcialidade de todo o processo;
- Assegure que os resultados das auditorias sejam relevantes para a gestão da empresa e todo o processo de auditorias e os seus resultados sejam documentados com evidência;

A administração da empresa deve rever o SGSI da mesma em intervalos para assegurar a sua sustentabilidade e eficácia. A avaliação da gestão deve ter em consideração o estado das avaliações anteriormente feitas, mudanças nos problemas interiores e exteriores relevantes ao SGSI e que o *feedback* na performance da segurança de informação inclua tendências em ações corretivas e que não estejam em conformidade, nos resultados de monitorização e medição, nos resultados das auditorias e se os objetivos da segurança de sistemas foram cumpridos.

A avaliação da gestão também deve ter em consideração o *feedback* das partes interessadas, das avaliações aos resultados de riscos e o estado do plano de tratamento de riscos, e as oportunidades para aumentar o melhoramento. O resultado da avaliação da gestão deve incluir decisões relacionadas com o melhoramento contínuo e mudanças relativas ao SGSI, sendo que toda a documentação em relação resultados da avaliação da gerência deve ser guardada como evidência.

A empresa deve, quando uma não conformidade ocorrer, reagir à mesma e, quando aplicável, tomar ações para controlar e/ou corrigir, lidando com as suas consequências. Deve avaliar a necessidade de tomar ações para que esta não aconteça mais nenhuma vez em lado algum, revendo a não conformidade, determinando as suas causas e existem-se semelhantes que possam ocorrer. A empresa deve também decidir quais as ações necessárias, rever se essas foram eficazes e fazer mudanças ao SGSI se necessário.

As ações corretivas devem ser apropriadas em relação a não conformidade encontrada. A empresa deve reter toda a documentação relativamente à natureza das não

conformidades, as ações tomadas em relação às mesmas e os resultados de todas as medidas de correção tidas como evidência. A empresa deve continuar a promover a sustentabilidade e eficácia do SGSI.

2.7.6 *ISO 27019:2017*

A ISO 27019:2017 [23] fornece orientação baseada na ISO 27002:2013 aplicada a sistemas de controlo de processo usados pela indústria de serviços públicos de energia para controlar e monitorizar a produção ou geração, transmissão, armazenamento e distribuição de energia elétrica, gás, óleo e calor, e para o controlo dos processos de suporte associados. As orientações incluídas na documentação são:

- controlo central e distribuído de processos, tecnologia de monitorização e automação, bem como sistemas de informação utilizados para sua operação, como dispositivos de programação e parametrização;
- controladores digitais e componentes de automação, como PLCs, incluindo sensores digitais e elementos atuadores;
- todos os outros sistemas de informação de suporte usados no domínio de controlo de processo, por exemplo, para tarefas suplementares de visualização de dados e para controlo, monitorização, arquivo de dados, registo do histórico, geração de relatórios e documentação;
- tecnologia de comunicação usada no domínio de controlo de processo, por exemplo, redes, telemetria e tecnologia de controlo remoto;
- componentes de AMI, por exemplo, medidores inteligentes;
- dispositivos de medição, por exemplo, para valores de emissão;
- sistemas digitais de proteção e segurança, por exemplo, *relays* de proteção, PLCs de segurança, mecanismos reguladores de emergência;
- sistemas de gestão de energia, por exemplo, de DER, infraestruturas de carregamento elétrico, em habitações particulares, edifícios residenciais ou instalações de clientes industriais;
- componentes distribuídos de ambientes de *smart grid*, por exemplo, em redes de energia, em residências particulares, edifícios residenciais ou instalações de clientes industriais;

- todos os *softwares*, *firmware* e aplicações instalados nos sistemas mencionados acima, por exemplo, aplicações *Distribution Management System* ou *Outage Management System*;
- sistemas de manutenção remota para os sistemas acima mencionados;

Este *standard* não se aplica ao domínio de controlo de processo de instalações nucleares, sendo que este domínio é coberto pelo *standard* IEC 62645.

Este *standard* também inclui um requisito para adaptar os processos de avaliação e tratamento de riscos descritos na ISO 27001:2013 às orientações específicas do setor de serviços públicos de energia descritos neste documento.

3

TRABALHOS RELACIONADOS

Este capítulo está relacionado aos trabalhos pesquisados para a criação do roteiro, dando uma introdução aos artigos pesquisados, o que eles contêm e o material útil usado.

3.1 ROTEIRO PARA CAPACIDADES MÍNIMAS DE CIBERSEGURANÇA

Segundo [24], os incidentes de cibersegurança têm-se mostrado mais frequentes e complexos. Face a isto, interessa preparar a governação interna das empresas, no sentido de elevarem o nível da sua cibersegurança, tendo em conta as suas diversas vertentes.

Para apoiar o desenvolvimento de valências mínimas em cibersegurança, sobretudo nas Pequenas e Médias Empresas e, num âmbito mais alargado, na generalidade das empresas no panorama nacional, foi definido um conjunto de capacidades — técnicas, humanas e processuais — que constituem uma base harmonizada e desejável nesta matéria.

Pretende-se assim proporcionar um instrumento que aumente o nível da empresa no domínio da governação de segurança de informação, focado nas competências e capacidades, incluindo ao nível de recursos humanos, para identificar ameaças, percebê-las e reagir face aos riscos do ciberespaço e das atividades em rede.

Foi assim estabelecido o Roteiro para Capacidades Mínimas em Cibersegurança, constituído por cinco fases para as empresas integrarem o ecossistema nacional de cibersegurança, criando, simultaneamente, condições para uma melhoria sustentada e coerente dessas capacidades.

Este Roteiro deve ser utilizado como um instrumento complementar ao Quadro Nacional de Referência para a Cibersegurança, [25]. Este último é um documento orientador, que aborda os diversos vetores relacionados com a problemática da segurança nas empresas, seguindo as linhas gerais de normativos como as da família ISO/IEC 27000 ou as que se encontram sob a chancela da NIST. Pretende-se que o Roteiro constitua, no quadro da realidade das Pequenas e Médias Empresas, a

concretização prática das diretrizes que faça sentido implementar, tendo em conta quer a limitação de recursos destas empresas, quer aqueles que devem ser os seus requisitos do ponto de vista da proteção dos seus ativos.

Este documento permitirá desenvolver gradualmente o nível de cibersegurança nas várias empresas. O CNCS disponibiliza um conjunto de instrumentos para ajudar ao desenvolvimento de algumas capacidades. A caraterização destes instrumentos, a sua forma e o seu âmbito podem ser consultados no sítio da Internet do CNCS. Os restantes custos envolvidos na execução deste Roteiro são da responsabilidade da empresa, como, por exemplo, a possível aquisição de ferramentas, instrumentos ou contratação de recursos humanos.

Ao longo das cinco fases aqui caracterizadas, as ações que se elencam visam a capacitação da empresa com recursos próprios. Deve referir-se, no entanto, que, dependendo da análise de risco e eficiência ao nível de custos, resultados equivalentes poderão ser obtidos recorrendo à subcontratação de serviços, equipamentos ou mesmo de recursos humanos.

Relativamente às ações aqui preconizadas, deve acrescentar-se que, mesmo nos pontos onde não é referida esta via explicitamente, a opção pela subcontratação ou externalização de soluções pode e deve ser equacionada pela empresa como alternativa válida à implementação com recursos internos. Também no domínio da intervenção humana, o mercado oferece soluções de resposta a incidentes, deteção e monitorização contínua de segurança.

A importância da análise de risco na tomada de decisões sobre a forma de implementação permite procurar o equilíbrio entre eventuais desvantagens financeiras e logísticas em dispor de meios próprios com potenciais impactos na segurança na totalidade, ou optar-se pela externalização ou subcontratação. Esses potenciais impactos poderão advir da dependência de empresas externas, eventuais riscos de confidencialidade e problemas de portabilidade. É importante que estas decisões sejam tomadas conscientemente pela empresa, tendo presente a criticidade dos ativos de informação que protege, no enquadramento das suas capacidades financeiras.

3.2 *GUIDE TO INDUSTRIAL CONTROL SYSTEMS SECURITY*

Segundo [26], este documento fornece orientação sobre como proteger os ICS, incluindo Sistemas SCADA, DCS e outras configurações do sistema de controlo,

como PLCs, fazendo face aos seus requisitos exclusivos de desempenho, confiabilidade e segurança.

Fornece também uma visão geral do ICS e topologias de sistema típicas, identifica ameaças e vulnerabilidades típicas a esses sistemas e fornece contramedidas de segurança recomendadas para mitigar os riscos associados aumentando a cibersegurança dos mesmos. Este documento é a revisão do documento e conjunto de regras do NIST SP 800-53 Rev.4 direcionado especificamente para ICS e a sua segurança, que inclui os sistemas de energia.

Ele é composto pelas seguintes secções:

- Secção 1 providencia uma visão geral do ICS que inclui comparações entre sistemas IT e ICS;
- Secção 2 providencia uma discussão sobre a gestão e avaliação de riscos em ICS;
- Secção 3 providencia uma visão geral do desenvolvimento e implantação de um programa de segurança ICS para mitigar o risco das vulnerabilidades identificadas;
- Secção 4 providencia recomendações para a integração de segurança em arquiteturas de rede normalmente encontrados no ICS;
- Secção 5 providencia um resumo dos controlos de gestão, operacionais e técnicos identificados na Publicação Especial NIST 800-53, Controlos de Segurança e Privacidade para Sistemas de Informação Federais e Organizações, e fornece orientação inicial sobre como esses controlos de segurança se aplicam ao ICS;

Estes controlos são direcionados para sistemas industriais, mas podem ser aplicados também em contexto de empresas do sector energético.

3.3 ENERGY SECTOR ASSET MANAGEMENT FOR ELECTRIC UTILITIES, OIL & GAS INDUSTRY

Referido no trabalho [27], o *National Cybersecurity Center of Excellence* (NCCoE) que se inclui no NIST localizado nos Estados Unidos da América, construiu um ambiente de laboratório para demonstrar como as empresas do sector energético podem fortalecer as suas práticas de gestão de ativos de OT aproveitando capacidades que já podem existir no ambiente operacional ou pela implementação de novas capacidades.

Como as empresas do setor energético e a indústria de petróleo e gás são algumas das infraestruturas críticas do país, a incapacidade ou destruição de ativos, sistemas e redes no setor de setor energético têm sérios efeitos negativos na economia, na saúde pública e na segurança. À medida que os ICS no setor energético tornam-se mais interconectados, as vulnerabilidades em ativos e processos OT são alvos de agentes maliciosos.

Um desafio para as empresas do setor energético é manter um inventário de ativos atualizado. Não tendo este inventário atualizado implica que não se poderá proteger o que não é visto ou o que não é conhecido. Sem uma solução eficaz de gestão de ativos, empresas que desconhecem os ativos da infraestrutura podem-se expor a riscos de cibersegurança.

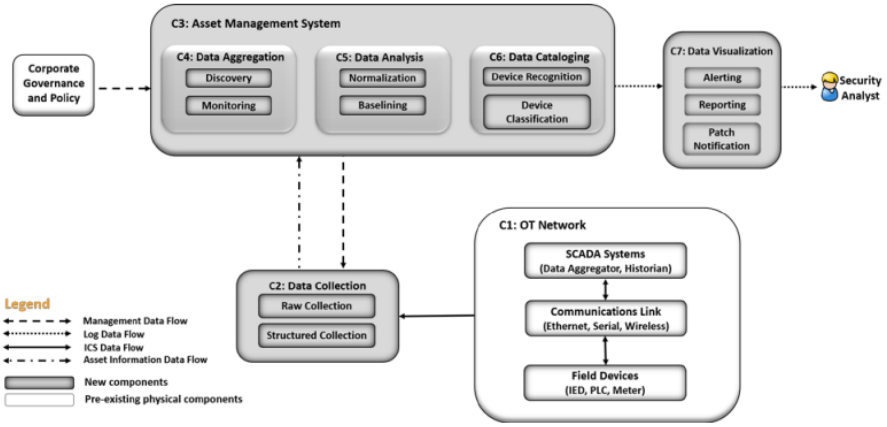


Figura 2: Arquitetura de Gestão de Ativos [27]

Como demonstrado na Figura 2, este *NIST Cybersecurity Practice Guide* fornece etapas detalhadas de como as empresas do setor energético podem identificar e gerir ativos OT e detetar riscos de cibersegurança associados a eles.

3.4 *Framework for Improving Critical Infrastructure Cybersecurity*

Segundo [28], para a criação de uma estrutura para melhorar a cibersegurança da infraestrutura critica criado pelo NIST:

Esta *Framework* concentra-se na orientação das atividades de cibersegurança e considera os riscos de segurança como parte dos processos de gestão de riscos da empresa. A *Framework* consiste em três partes:

- Núcleo da estrutura;

- Camadas de implementação;
- Perfis de estrutura;

O *Framework Core* é um conjunto de atividades, resultados e referências informativas comuns em todos os setores de infraestruturas críticas. Elementos deste fornecem orientação detalhada para o desenvolvimento de*frameworks* organizacionais individuais. Através do uso destas *frameworks*, a estrutura ajudará uma empresa a alinhar e priorizar a sua segurança e atividades cibernéticas com os seus requisitos de negócios, tolerâncias de risco e recursos.

Os níveis fornecem um mecanismo para as empresas visualizarem e intendam as características da sua abordagem para gerir o risco de cibersegurança. Apesar deste documento ter sido desenvolvido para melhorar a gestão de riscos de cibersegurança em infraestruturas críticas, a *Framework* pode ser utilizada por empresas de qualquer setor.

Esta permite às empresas — independentemente do tamanho, grau de risco de cibersegurança ou sofisticação da cibersegurança — aplicar os princípios e as melhores práticas de gestão de riscos para melhorar a segurança e a resiliência.

Ela fornece uma estrutura de empresa comum para várias abordagens para cibersegurança, reunindo padrões, diretrizes e práticas que são eficazes atualmente, sendo que, pode servir como um modelo para a cooperação internacional no fortalecimento da cibersegurança em infraestrutura crítica, bem como noutros setores.

Esta oferece uma maneira flexível de abordar a cibersegurança, incluindo o efeito da cibersegurança nas dimensões físicas, cibernéticas e de pessoal. É aplicável a empresas que dependem de tecnologia, se o seu foco de cibersegurança é principalmente em IT, sistemas de controlo industrial, sistemas ciberfísicos ou dispositivos conectados mais geralmente, incluindo a Internet das Coisas. Finalmente, ela pode auxiliar as empresas a abordar a cibersegurança, ao afetar a privacidade de clientes, funcionários e outras partes.

Além disso, os resultados da Estrutura servem como metas para o desenvolvimento da força de trabalho e atividades de evolução.

3.5 ROADMAP FOR PHOTOVOLTAIC CYBER SECURITY

Segundo o relatório [1], redigido para o aumento da cibersegurança fotovoltaica nos Estados Unidos da América: Energia segura e resiliente é fundamental para a prosperidade dos Estados Unidos. Enquanto a experiência e sofisticação dos adversários

cibernéticos crescerem, o mesmo deve acontecer com o sistema de energia dos EUA, as suas defesas, consciência situacional e estratégias de resposta e recuperação. Na Figura 3, são indicados alguns projetos financiados pelo departamento de Energia dos Estados Unidos da America, demonstrando o seu compromisso para uma maior cibersegurança no sector.

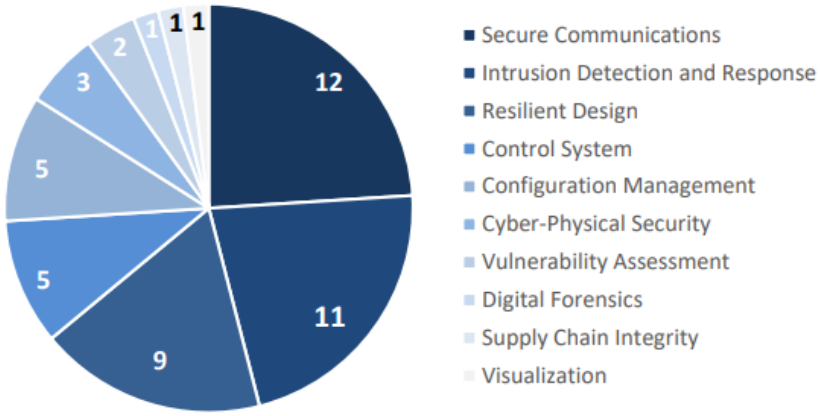


Figura 3: Projetos financiados pelo departamento de Energia dos EUA por área [1]

Tradicionalmente, os sistemas de energia foram operados com canais de comunicação dedicados para grandes geradores e ativos de propriedade da concessionária, mas agora há uma maior dependência de sistemas fotovoltaicos para fornecer energia geração.

Os sistemas fotovoltaicos comunicam com agregadores e outros operadores de rede por meio da *internet* pública, pelo que a superfície de ataque do sistema de energia se tenha expandido significativamente. No mesmo tempo, os sistemas de energia solar são equipados com uma variedade de funções de suporte à rede que, se controladas ou programadas incorretamente, apresentam um risco de distúrbios do sistema de energia. Este documento é um roteiro de cinco anos destinado a traçar um caminho para melhorar a cibersegurança para comunicações habilitadas de sistemas fotovoltaicos com funções e responsabilidades claras para o governo, desenvolvimento de padrões, empresas, fornecedores de sistemas fotovoltaicos e operadores de rede.

Um roteiro de cinco anos para cibersegurança fotovoltaica é apresentado com recomendações para atrair as partes interessadas, pesquisa e desenvolvimento, desenvolvimento de padrões e melhores práticas. Este roteiro orienta políticas nacionais e locais, padrões e políticas públicas e privadas e investimento para

melhorar a resiliência do sistema de energia dos EUA, fortalecendo as redes de controlo fotovoltaico, desenvolvendo e implementando tecnologias de deteção e preparando-se para responder rapidamente a ameaças cibernéticas. Através da implementação coletiva dessas tecnologias, a segurança da energia fotovoltaica e os sistemas de controlo podem ser fortalecidos sem comprometer o desempenho da rede.

A Figura 4 demonstra como a segurança nas DER pode ser assegurada usando *IEC 61850* e *IEC 62351* para a aplicação de várias políticas para o aumento da cibersegurança nas DER.

A liderança sustentada em cibersegurança e comprometimento das partes interessadas é necessária para melhorar continuamente os equipamentos e redes fotovoltaicas, criar padrões eficazes, manter trocas de informações público-privadas e apoiar os esforços nas pesquisas e desenvolvimentos governamentais e comerciais. Manter o impulso positivo é responsabilidade de todas as partes interessadas. Como próximo passo, as recomendações fornecidas neste documento devem ser priorizadas para direcionar as partes interessadas em investimento de atividades de alto impacto.

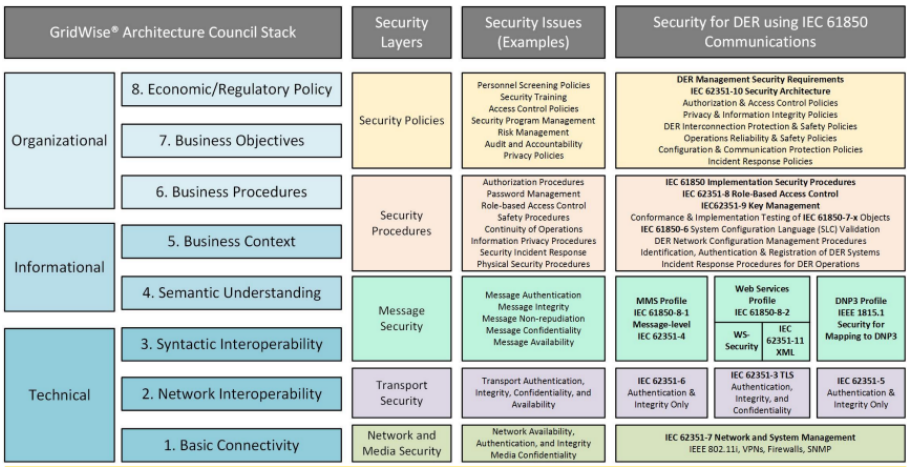


Figura 4: Segurança para Recursos de Energia Distribuída usando comunicações IEC 61850 e IEC 62351 [1]

3.6 CIBERSEGURANÇA NUMA REDE DE ENERGIA: ESTADO DA ARTE

Segundo [29], neste estudo é demonstrado o estado da arte numa rede de energia e da tecnologia de *smart grids*, apresentando as suas vulnerabilidades, soluções para intrusões cibernéticas e ameaças não resolvidas.

Os sistemas de comunicação entre subestações tradicionais usam apenas cabos de cobre que apenas permitem um par de dispositivos, mas aplicando uma comunicação digital usando *Ethernet* reduz custos, aumenta a eficiência e permite múltiplas comunicações.

A arquitetura de comunicação das *smart grids* é feita usando um sistema de transmissão que entrega energia a centros remotos, tendo estas várias interações que afetam a sua estabilidade. Os sistemas de tecnologia de informação e comunicação suportam a monitorização e controlo no sistema de energia. Para recolher as medições e dados de estados são usados os sistemas SCADA e com essa informação um sistema de gestão de energia determina ações.

O *design* dos sistemas de automação de subestações tem vantagens, como, por exemplo, a redução de custo de engenharia devido à integração de comunicações*Ethernet*, aumenta a interoperabilidade em vários produtores e minimiza o impacto quando a topologia de comunicações é alterada.

A unidade de medição de fasor aumenta a observabilidade do sistema de energia e estes dados são enviados para um centro de controlo e usando várias destas aplicações aumenta a confiabilidade da rede.

Para proteção desta rede são usadas *firewalls*, IDS e mecanismos de proteção criptográfica. Como principal componente no controlo de sistemas, a SCADA é o alvo primário para ameaças, sendo que há vários pontos de entrada para atacantes numa *smart grid*.

Para assegurar confiabilidade as *smart grids* tem de seguir várias regulações e *standards* internacionais.

Potenciais ameaças nas redes incluem a sincronização dos dados da *smart grid*, vulnerabilidades na comunicação *wireless*, validação dos dados recolhidos pelos IDS, ataques coordenados e falhas relacionadas com o fator humano.

3.7 *RECOMMENDED FUNCTIONALITIES FOR IMPROVING CYBERSECURITY OF DISTRIBUTED ENERGY RESOURCES*

Segundo [30], este artigo fala sobre funcionalidades avançadas dos recursos de energia distribuídos (DER) requeridos pela *Institute of Electrical and Electronics Engineers* (IEEE) para a interconexão da DER na rede, vulnerabilidades e o seu impacto nas operações da rede de distribuição inteligente e recomendações de funcionalidade para melhorar a cibersegurança.

As grelhas de energia tradicionais não estão preparadas para múltiplas fontes distribuídas nem para que o fluxo de energia seja bidirecional.

Deste modo foram criadas estruturas modernas para gestão de DER. Se o modo avançado de um destes for comprometido, os impactos para a rede elétrica podem ser devastadores, sendo necessário identificar as suas funcionalidades e vulnerabilidades.

A funcionalidade de um moderno DER inclui o modo de fator de potência constante, modo para limitação energética ativa, modo de energia reativa constante, modo de energia reativa à tensão, modo de energia reativa de energia ativa, modo de tensão ativa e o modo de queda de frequência.

As consequências de um ataque dependem sempre se o atacante consegue controlar um ou mais DER e quais os modos afetados referidos anteriormente.

As consequências dos ataques a estes modos podem incluir alterações da frequência, aumento ou diminuição de voltagens, redução da eficiência da rede, sobrecarga dos ativos da rede, desconexão dos sistemas DER e perda de carga ou danos aos dispositivos elétricos.

Devem usar-se mecanismos de segurança para a deteção de ataques que possam afetar os DER sendo que as vulnerabilidades e/ou ataques mais comuns incluem *man-in-the-middle*, *replay*, espionagem, *spoofing* por certificados de segurança, negação de serviço, violação de privilégio mínimo e certificados de força bruta, mas há cada vez mais ataques diferentes que afetam estes sistemas.

Para o aumento de segurança destes sistemas foram criados vários *standards* e regras para aumentar a segurança. Com estes *standards* e regras em mente, foram implementadas várias soluções para proteger os DER como sistemas operativos mais robustos, possível reversão de atualizações de firmware caso haja atualizações com falhas conhecidas e graves, implementação de autenticação, gestão de *passwords*, implementação de *Transport Laver Security* (TLS), lista de revogação de certificados, expiração de certificados, renegociação de sessões e estudo dos fornecedores de componentes.

3.8 A "REVIEW" ON CYBERSECURITY IN SMART LOCAL ENERGY SYSTEMS: REQUIREMENTS, CHALLENGES, AND STANDARDS

Segundo [31], o *smart local energy system*(SLES) é considerado um caminho promissor que facilita uma operação eficaz e localizada, beneficiada pela complexa informação e infraestruturas de TIC e IoT. Sendo uma parte da infraestrutura

crítica, é importante não só colocar a deteção eficaz e gestão para lidar com possíveis problemas de cibersegurança, mas também exigem números consideráveis de padrões para garantir a segurança do sistema de IoT para minimizar os riscos.

Este estudo revê os padrões existentes, investiga como a compatibilidade com o desenvolvimento de SLES e identifica a área a ser focada no futuro. Embora os padrões existentes e os protocolos sejam altamente fragmentados, as nossas descobertas sugerem que muitos deles podem atender aos requisitos dos aplicativos e infraestruturas do sistema de energia local inteligente. Além disso, muitos padrões foram introduzidos para proteger a segurança da informação e a privacidade pessoal devido à sua importância crescente.

Neste relatório, é feita uma revisão dos padrões técnicos existentes que abordam questões de cibersegurança. Nas descobertas sugerem que um número considerável de padrões ou protocolos pré-existentes atenderiam aos requisitos de aplicação e infraestrutura do sistema de energia local inteligente. Os padrões existentes são altamente fragmentados e específicos para determinada indústria, enquanto algumas estruturas de segurança fornecem diretrizes gerais aplicáveis a qualquer indústria ou empresa sem detalhes técnicos.

A maioria dos padrões foca-se apenas em proteger um ou alguns componentes, ou recursos de segurança no sistema pelo projeto. Também foi descoberto que a segurança da informação está a tornar-se cada vez mais importante, e muitos padrões são introduzidos para proteger segurança da informação e privacidade. No entanto, o desenvolvimento bem-sucedido do sistema de energia local inteligente ainda requer mais esforço de vários lados.

Com base nas descobertas e sugestões produzidas a partir desta pesquisa, é importante estender a pesquisa e investigar mais como estas podem contribuir para a conceção e operação de sistema de energia local inteligente. O trabalho futuro proposto neste documento concentrar-se-á em propor uma estrutura para a deteção e tratamento para garantir a cibersegurança do sistema de energia local inteligente. A primeira parte da estrutura resulta numa ferramenta de avaliação que visa identificar as potenciais vulnerabilidades, ameaças e ataques de cibersegurança.

A avaliação sobre as ameaças será determinada por várias métricas, como o tipo de ameaças, localização na arquitetura cibernética e física e partes interessadas responsáveis. A avaliação irá resultar numa resposta estratégica. As métricas de ameaças são usadas para priorizar tarefas com base no nível de urgência e gravidade da ameaça. Soluções relevantes e técnicas são fornecidas para responder e prevenir

as potenciais ameaças no ciberespaço, dispositivos físicos ou camadas de utilidade para garantir a operação com cibersegurança.

3.9 CYBERSECURITY AND THE SMARTER GRID

Segundo [15], a confiabilidade continua a ser um princípio fundamental dos esforços de modernização da rede, mas no mundo de hoje, a confiabilidade requer cibersegurança. Este artigo discute várias empresas do setor de energia que projetam cibersegurança na rede inteligente com a visão de sobreviver a um incidente cibernético enquanto mantém funções críticas de fornecimento de energia. Algumas das empresas descritas neste são as empresas de cibersegurança *FirstEnergy*[1] usando o NIST 800-53, a *Duke Energy Progress's EnergyWise Initiatives*[2] e *Northern Virginia Electric Cooperative*[3].

As parcerias do setor de energia permitem um maior desenvolvimento de medidas de cibersegurança, devido à junção de recursos e partilha de informação e a criação de protocolos, procedimentos e mecanismos que aumentam a segurança.

Para além de incluir as parcerias, inclui medidas de cibersegurança já implementadas pelo sector energético e os pontos principais na gestão, monitorização, proteção e controlo de *smart grids*.

3.10 RESEARCH ON CYBERSECURITY STRATEGY AND KEY TECHNOLOGY OF THE WIND FARMS' INDUSTRIAL CONTROL SYSTEM

Segundo [32], devido a haver um foco na funcionalidade desprezando a segurança, existem muitas ameaças ocultas no sistema de controlo industrial de parques eólicos (ICS-WF), como más configurações de IPs, falha na deteção e eliminação de vírus, que são propensos a invasão ilegal e ataque do ciberespaço. Esses acessos não autorizados são bastante prejudiciais para a operação estável dos parques eólicos e da rede elétrica regional. Portanto, investigando a situação atual de segurança e as necessidades do ICS-WF, analisando as características da arquitetura e comunicação interna do ICS-WF e integrando as ideias da proteção classificada de cibersegurança, este artigo propõe uma nova estratégia de cibersegurança personalizada para o ICS-WF.

1 https://firstenergycorp.com
2 https://duke-energy.com
3 https://novec.com

Também foi introduzida uma tecnologia de deteção de intrusão anómala para ICS-WF, desenvolvida com base em modelos estatísticos de características de rede de parques eólicos. Por fim, combinado todo esse trabalho com o ataque de segurança de rede e exercício de defesa no laboratório de simulação de segurança de controlo industrial de parques eólicos, esta pesquisa formula uma solução de proteção abrangente tridimensional para ICS-WF, que melhora significativamente o nível de cibersegurança de ICS-WF.

3.11 *OPERATIONAL TECHNOLOGY CYBERSECURITY FOR ENERGY SYSTEMS*

Segundo [33], turbinas eólicas, painéis solares, sistemas de controlo de edifícios e sistemas SCADA são exemplos de sistemas OT e são relevantes para como os EUA produzem, armazenam e gerem energia. Muitos desses sistemas OT possuem componentes ou conexões de IT. No entanto, cada um deles apresenta vulnerabilidades, riscos e consequências significativamente diferentes no que se refere à sua proteção. Este documento apresenta a importância dos sistemas OT, riscos e tipos de ataques a estes sistemas. Também apresenta algumas medidas para a melhoria da cibersegurança desses sistemas.

4

ANÁLISE

Neste capítulo descreverei os artigos que usei para redigir este trabalho, que peças retirei destes artigos e o porquê do uso destas para a redação do mesmo.

4.1 ROTEIRO PARA CAPACIDADES MÍNIMAS DE CIBERSEGURANÇA

O Roteiro de Capacidades Mínimas de Cibersegurança [24] servirá como base para a construção do roteiro de capacidades mínimas de cibersegurança no sector energético. Será composto por fases semelhantes e terá algumas sugestões parecidas ao roteiro devido às organizações usarem muitos produtos de TI mas também terá soluções, passos e sugestões especifica ao sector energético, nomeadamente com a parte OT entre outros. Os tópicos que são semelhantes estão na Figura 5, onde é feita a comparação entre o roteiro de Capacidades Mínimas de Cibersegurança redigido pelo CNCS e o roteiro proposto.

4.2 *GUIDE TO INDUSTRIAL CONTROL SYSTEMS SECURITY*

Este documento [26] é um guia para a implementação de cibersegurança para sistemas industriais. Por conseguinte, foram utilizadas as definições dos componentes explicados como os sistemas SCADA, DCS e PLCs e como é feita a gestão de risco num ICS.

Também foram retiradas ideias de como deve ser organizada a arquitetura de segurança, a sua composição, desde firewalls, segmentação e segregação da rede, autenticação e autorização, monitorização e várias recomendações para a melhoria da mesma.

Figura 5: Comparação dos Roteiros

4.3 ENERGY SECTOR ASSET MANAGEMENT FOR ELECTRIC UTILITIES, OIL & GAS INDUSTRY

Este documento [27], demonstra uma implementação de teste de tecnologias para a descoberta e gestão de ativos do sector energético. Esta implementação pode ser usada como base para as fases 1 e 2 onde é preciso fazer a descoberta dos ativos da empresa, a sua priorização e a sua monitorização. Sendo que não apresenta soluções para tomar ações caso haja um ataque malicioso, o facto de possibilitar que a empresa tenha visibilidade e monitorização quase completa dos seus ativos já permite aumentar bastante a cibersegurança e posteriormente tomar ações quando necessário.

Foi usado na fase 1 uma imagem, Figura 9, que representa um exemplo que pode ser usado como arquitetura de alto nível, pois será um exemplo parecido ao de uma empresa real deste sector devido a ter vários locais remotos de produção de energia. Com este exemplo terão uma ideia de que ativos devem ser monitorizados.

Na fase 2, foi usada uma imagem (Figura 10), que representa um exemplo de uma arquitetura de referência, com todas as tecnologias e fluxos de dados que poderão ser usados para a construção de uma arquitetura. Estas peças permitem dar uma maior ideia de como será construída a arquitetura da empresa relativamente à gestão e monitorização de dados, sendo uma boa fundação e com espaço de implementação para mais passos descritos no roteiro.

4.4 FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

Sendo o sector elétrico um sector crítico, foram usadas várias secções deste documento [28]. A *framework* deste documento, *Identify, Protect, Detect, Respond and Recover*, coincide com as 5 fases propostas neste documento, sendo que foram usadas várias categorias do *Framwork Core*. Foram usadas estas categorias por coincidirem com as fases do roteiro, pelo facto de ser uma arquitetura que melhora as capacidades de cibersegurança em sectores críticos, fazendo sentido a sua adição à proposta.

4.5 *ROADMAP FOR PHOTOVOLTAIC CYBER SECURITY*

Neste roteiro [1] foram obtidos mais dados relacionados com ataques já realizados ao sector energético e as suas consequências. Foram obtidos também processos para aumentar a cibersegurança em sistemas fotovoltaicos. Estes processos, apesar de serem focados a uma parte específica do sector energético, foram uma base para a construção das fases do roteiro como mostrado na Figura 6.

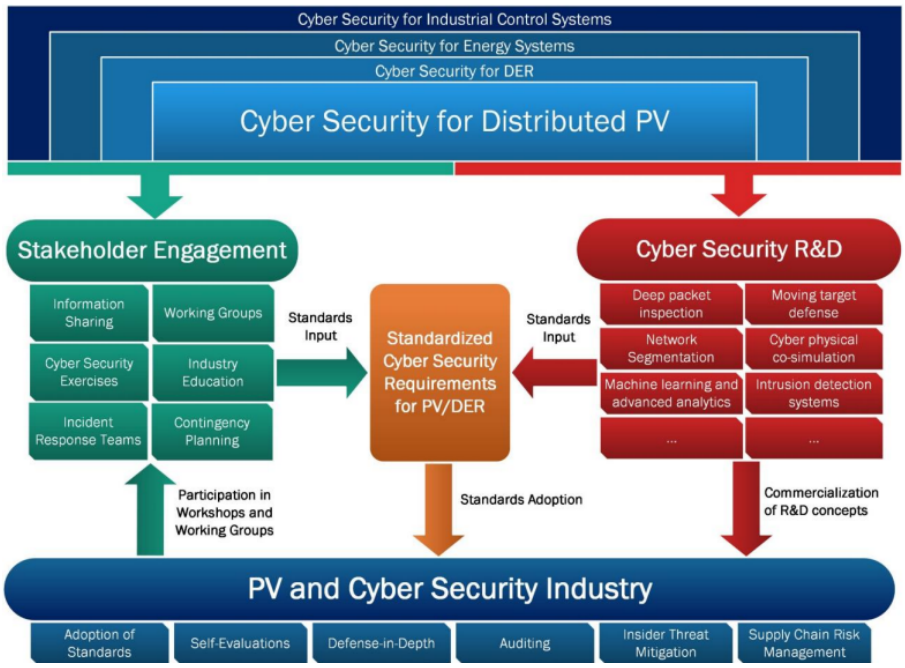


Figura 6: Processos para obtenção da cibersegurança em sistemas fotovoltaicos descritos [1]

Foram descobertas as principais barreiras para aplicação da cibersegurança no sector. Isso permitiu acrescentar um contexto ao trabalho, o que é relevante para compreender o plano e as dificuldades de implementação. Foram também extraídos alguns *standards* usados pelo sector energético para a sua implementação no roteiro. Estes são essenciais para a implementação e manutenção de um maior nível de cibersegurança na empresa e dos seus ativos.

4.6 CIBERSEGURANÇA NUMA REDE DE ENERGIA: ESTADO DA ARTE

Este artigo [29], demonstra o funcionamento da rede de energia, os seus componentes, vulnerabilidades, soluções e pesquisas já feitas para tentar colmatar estas vulnerabilidades. Tendo estes conceitos em conta, foi usado neste documento as

tecnologias usadas tanto para o funcionamento da rede como para a aplicação de cibersegurança na mesma e vulnerabilidades conhecidas.

As tecnologias retiradas ajudam a perceber como funciona a rede, como é feita a monitorização da mesma e técnicas para a deteção e resposta rápida a ataques à mesma. Algumas destas tecnologias são os Sistemas SCADA, PMU, *Advanced metering infrastructure*(AMI), DER, *Distribution Automation* ou *Anomaly detection systems*.

Ao sabermos das vulnerabilidades já conhecidas e vetores de ataque comuns temos um maior conhecimento de aonde devem aplicadas maiores medidas de monitorização e prevenção de intrusões. Algumas dessas vulnerabilidades são as comunicações *wireless*, o fator de erro humano, ataques coordenados ou a sincronização dos dados.

4.7 RECOMMENDED FUNCTIONALITIES FOR IMPROVING CYBERSECURITY OF DISTRIBUTED ENERGY RESOURCES

Este documento [30], demonstra como funciona os recursos distribuídos de energia, que proteções já estão implementadas, as suas vulnerabilidades e métodos como aplicar maior cibersegurança. Segundo [34], a energia elétrica em Portugal vem de várias fontes diferentes como eólica, hidroelétrica, fóssil ou solar, este documento integra-se bem na formulação do roteiro.

As funcionalidades e vulnerabilidades serão importantes analisar na fase 1, em que se fazem a recolha dos ativos, podendo imediatamente visualizar os mais críticos ou os mais vulneráveis. Descreve vários *standards* e métodos para garantir a cibersegurança que foram implementadas nas fases 2 e 3 do roteiro.

4.8 A REVIEW ON CYBERSECURITY IN SMART LOCAL ENERGY SYSTEMS: REQUIREMENTS, CHALLENGES, AND STANDARDS

Este documento [31], demonstra o funcionamento de um sistema de energia local inteligente, as suas vantagens, os riscos para este, *standards* e tecnologias usadas para este tipo de sistema.

Apesar de ser um caso mais específico no sector energético, os riscos de cibersegurança que afetam este sistema, afetam também várias áreas deste sector. Sabendo isso, podem se aplicar os *standards* como algumas das tecnologias deste sistema.

4.9 *CYBERSECURITY AND THE SMARTER GRID*

Este documento [15], demonstra alguns métodos e normas usadas para garantir a cibersegurança numa rede inteligente.

Foram usados vários conteúdos relacionados com os sistemas SCADA, EMS, AMI e unidades de medição fasorial, ao serem tecnologias fulcrais e essenciais para a monitorização e controlo do fluxo de energia na rede elétrica, sendo que serão mencionados nas várias etapas da proposta.

4.10 *RESEARCH ON CYBERSECURITY STRATEGY AND KEY TECHNOLOGY OF THE WIND FARMS' INDUSTRIAL CONTROL SYSTEM*

Este documento [32], demonstra vários métodos de proteção de um parque eólico que podem também ser usados no sector em geral, como a utilização de IDS/IPS, antivírus, sistemas de monitorização da rede, entre outros. Alguns desses métodos foram adicionados à proposta pela sua pertinência devido a esta pesquisa ser sobre uma subsecção do sector energético.

4.11 *OPERATIONAL TECHNOLOGY CYBERSECURITY FOR ENERGY SYSTEMS*

Neste documento [33], foram usadas algumas medidas de melhoramento da cibersegurança como controlo de acesso, gestão de atualizações e de ativos e endurecimento da rede, pois este apresenta medidas concretas que ao serem executadas por uma empresa do sector energético aumentam a sua cibersegurança.

5

METODOLOGIA

Neste capitulo será descrito a metodologia usada para a criação do trabalho, os passos e pesquisas, incluindo as palavras-chave usadas nas pesquisas e na redação do mesmo.

Foram usados os motores de pesquisa de artigos académicos *sciencedirect* e *google scholar* e o motor de pesquisa *Google* para pesquisa de notícias. Para parâmetros, foram usados os artigos mais recentes, com mais citações e a sua relevância, sendo usado como parâmetro de distinção o título dos artigos. Apenas foram feitas pesquisas na primeira página que dá conta de 25 artigos. Tendo em conta que os motores de pesquisa também vão mostrar pesquisas feitas anteriormente, também é um parâmetro de escolha e de resultados mostrados.

Sendo que o roteiro é relacionado com o sector energético, foram efetuadas pesquisas sobre soluções de cibersegurança já aplicadas no sector, usando as palavras-chave *cybersecurity smart grid*. Foram encontrados 2057 resultados, dos quais apenas foram selecionados 2 artigos por estes terem o título mais parecido ao procurado e após a sua leitura estes terem as informações necessárias para a continuação da pesquisa. Tendo obtido informações de várias tecnologias aplicadas no sector foram efetuadas pesquisas por estas com as palavras-chave:

- *SCADA* com 10977 resultados, em que foi escolhido 1 artigo por este ter a sua definição, como é composto e vários mecanismos de mitigação
- *WAMS and SCADA* com 239 resultados em que foi escolhido 1 artigo e rejeitado 1, pois 1 tinha a definição do WAMS e a sua comparação ao sistema SCADA e o rejeitado não se enquadrava no material necessário
- *Smart grids* com 79175 resultados em que foram escolhidos 2 por apresentarem a definição de uma e como é composta
- *Operational Technology* com 8380000 resultados em que foram escolhidos 2 por apresentarem o seu funcionamento, a suas aplicações e o seu uso em *smart grids*

- *Photovoltaic cybersecurity* com 20300 resultados em que foram escolhidos 2, um deles por já apresentar um roteiro para cibersegurança fotovoltaica e outro por apresentar várias práticas e *standards* a aplicar numa planta fotovoltaica.

Também foi necessário pesquisar os *standards*, leis e normas aplicadas no sector para ter um maior contexto, pois a empresa que irá seguir este roteiro também terá que aplicar e seguir os mesmos. Para isto foi pesquisado pelas palavras-chave:

- Leis sector energético, com 26600 resultados em que foram escolhidos 2 por estes coincidirem com entidades reguladoras do sector e leis por eles redigidas, como, por exemplo, a ERSE
- *Eletric sector standards and norms*, com os resultados 251000 resultados e escolhidos 1 também por este coincidir com entidades reguladoras do sector
- *Regulatory bodies of the electric sector europe*, com 208000 resultados em que foram escolhidos 2 por estes contem as entidades reguladoras europeias e normas lançadas por estas, como, por exemplo, a ACER e a CEER

Tendo como base o roteiro de capacidades mínimas de cibersegurança redigido pelo CNCS para a redação da proposta e com várias sugestões para aumentar a cibersegurança, esta foi também uma das pesquisas feitas com 8320 resultados com a escolha do roteiro como resultado selecionado.

Foram também realizadas pesquisas sobre roteiros que possam já ter sido publicados por outras entidades, sendo que estes iriam diferenciar o roteiro proposto do roteiro do CNCS, podendo adicionar fases e passos específicos para o sector energético.

Para isto usamos as palavras-chave *Roadmap cybersecurity in electric sector* com 19700 resultados em que foram escolhidos 2 por representarem passos já tomados na indústria para melhorar a sua cibersegurança, tendo vários processos para a sua melhoria e *cyber security in operational technology devices* com 364000 resultados em que foram escolhidos 2, pois estes demonstravam o funcionamento de dispositivos OT, proteções já aplicadas e como aumentar a sua cibersegurança com vários métodos, sendo descartado 1, pois este já tinha dados retirados anteriormente de outros artigos e não se enquadrava na pesquisa necessária.

Também foi necessário fazer uma análise, tendo em contexto facto do setor energético ser crítico para a sociedade, quais casos de ciberataques já ocorreram e as suas consequências. Para isto foi efetuada uma pesquisa usando as palavras-chave *cyberattacks in electric sector* com 23000 resultados com 3 artigos escolhidos para

se ter uma maior perceção de vários ataques que possam ter ocorrido no sector energético e em sectores críticos.

Foi feita uma pesquisa sobre os elementos cibersegurança e como estes se integram com OT, pesquisando pelas palavras-chave *interoperability between OT e cibersegurança* com 26200 resultados e 1 artigo escolhido por dar exemplos da interoperabilidade dos sistemas. Também foi adicionada uma contextualização do que é a cibersegurança e alguns componentes que este contém pesquisando por *cybersecurity* em que foram escolhidos 3, onde 1 falava sobre a cibersegurança em infraestruturas critica, sendo no contexto da proposta. Os restantes 2 artigos davam contexto da cibersegurança, como é composta e que componente, métodos e normas estavam aplicadas no seu contexto.

Como a introdução não estava completa e precisava de fornecido contexto relativamente à importância de sector e o que fazia um sector crítico, foi pesquisado *why is electric sector critical* com 3170000 com 2 artigos escolhidos e 1 descartado. Os artigos escolhidos davam o contexto necessário relativamente à importância do sector e facto de este ser crítico enquanto o rejeitado não. Foi selecionado o *Sector Prime Series Energy* pois é um índice de desempenho das empresas de energia das S&P500,com 178000000 resultados usando 1 artigo onde é demonstrado a quota do mercado das empresas do sector, demonstrando a sua importância na sociedade. Com isto já havia terminado os capítulos da introdução, conceitos relacionados e trabalhos relacionados. No final foram escolhidos os documentos *Cybersecurity and the Smarter Grid*, *Energy Sector Asset Management For Electric Utilities for Oil and Gas Industry*, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, "Roteiro para Capacidades Mínimas de Cibersegurança" e *Roadmap for Photovoltaic Cyber Security* como peças essenciais para a construção do roteiro, pois estes tinham todas as peças necessárias para a criação do roteiro.

6

PROPOSTA

Esta secção é composta pela proposta do Roteiro de Capacidades Mínimas de Cibersegurança no Sector Energético, estando dividido por 5 fases. Cada fase é constituída pelos tópicos demonstrados na Figura 7. As fases darão à empresa

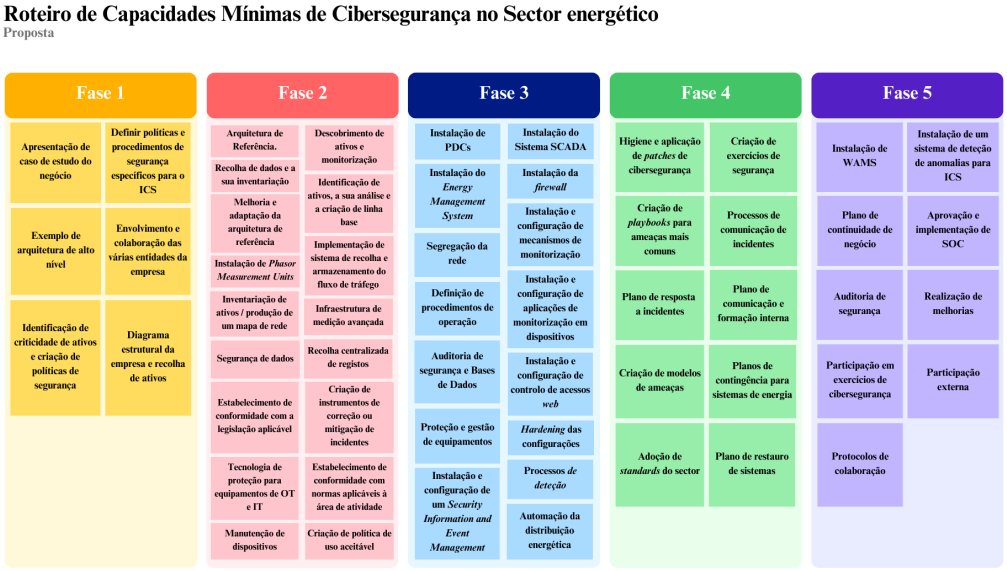


Figura 7: Fases da proposta do roteiro

mais segurança contra intrusões, uma troca de informações segura entre parceiros e uma capacidade de se reconfigurar para não permitir a falha de serviços. Além dessas capacidades, ela também será capaz de monitorizar intrusões, analisar dados analíticos e responder ativamente, guardando esses dados para uma futura análise ou para determinar atacantes. Cada fase terá tanto etapas relacionadas com o sector energético como etapas mais gerais devido à interligação de dispositivos OT e TI.

Na primeira fase deve haver uma cooperação entre todos os *stakeholders* da empresa, indivíduos interessados e com elevado nível de poder de decisão. Com esta cooperação deve-se decidir qual o quadro de ameaças que a empresa enfrenta, definir o valor relativo dos ativos e o seu grau de risco e definir áreas de segurança conforme esses ativos. Para atingir este objetivo devem ser criados grupos de trabalho das diferentes áreas na empresa para definir o seu grau de risco e a criticidade nessa mesma área. Deve haver partilha de informação de ameaças entre a empresa e

as agências governamentais como o CNCS para que esta esteja mais preparada caso haja ameaças já conhecidas. Esta partilha também deverá ser feita entre as empresas do sector para que estas ameaças sejam menos eficazes. Devem também ser identificadas todas as dependências externas que sejam geridas por terceiros, pois estas podem ser um ponto de ataques por não serem geridas diretamente pela empresa.

Na segunda fase será desenvolvida a arquitetura de segurança, onde serão aplicadas regras de controlo lógicas e/ou físicas nas várias áreas delimitadas no passo anterior. Esta fase deve aplicar estes controlos, para integrar nesta fase inicial uma segurança que possa detetar algumas tentativas de intrusão. Devem ser focados os controlos físicos às instalações e integrações entre TI e OT, por apresentarem maiores riscos e gerarem maiores consequências caso ocorra um ataque. Todos os dados obtidos por estes controlos devem ser guardados num repositório central para a sua consulta e posterior análise.

Na terceira fase será a implementação de um conjunto de técnicas e mecanismos de segurança para proteger a convergência entre os ativos de OT e IT. É também nesta fase que devem ser implementadas as capacidades, em conjunto com o responsável de segurança, de Identificar, Proteger, Detetar, Responder e Remediar, sendo que este objetivo é demonstrado num exemplo da estrutura a aplicar, segundo [28] na Figura 8. A empresa no fim desta fase deve ter capacidade que cumprir estas capacidades.

Os ativos mais importantes da empresa devem ser os primeiros a terem sido identificados e serem protegidos com a implementação de sistemas SCADA, HIDS, *Smart grids*, SIEM e SOAR. Com a ajuda destas tecnologias, deve haver uma avaliação contínua e automatizada dos riscos e das medidas técnicas desenvolvidas para reduzir a exposição a ciberataques. As medidas de proteção operacional são projetadas para defender a rede de controlo para que, se um adversário puder obter acesso às redes de controlo, a presença é detetada e ações maliciosas ou reconhecimento são dificultados.

Apesar de haver um maior controlo e maior capacidade de deteção, devem implementar-se contramedidas para aumentar a resiliência do sistema, estender o tempo e a dificuldade do ataque e minimizar o impacto no sistema se um ataque é bem-sucedido.

Na quarta fase, o objetivo é consolidar os conhecimentos obtidos nas fases anteriores, implementando procedimentos, normas e *standards*. Os procedimentos e normas serão o culminar do conhecimento obtido, enquanto os *standards* serão aqueles já

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figura 8: Função e Identificadores Únicos de Categorias [28]

usados pela indústria, como o ISO 27001 e 27002 ou *standards* da NIST. Deve ser também haver uma implementação das melhores pratícas usadas pela indústria para garantir a segurança.

Na quinta fase, o objetivo é a implementação de conceitos para empresas com mais capacidades, como a criação e desenvolvimento de um SOC, para que haja uma maior capacidade de monitorização e resposta da empresa. Deve também ser instalado o sistema WAMS, que tem maior capacidade de monitorização comparado com os sistemas SCADA. Estes sistemas, para além de permitirem uma maior capacidade, ajudam a melhorar os seus procedimentos e aumentar a comunicação de falhas de cibersegurança dentro e fora da empresa.

6.1 FASE 1

Nesta fase o objetivo será iniciar o processo da implementação do Roteiro de Capacidades Mínimas de Cibersegurança no Sector Energético. Este começa na apresentação do caso de estudo do negócio à administração, apresentando argumentos para a implementação do roteiro.

Deve haver o envolvimento e colaboração das várias entidades que compõem a empresa para haver uma maior abrangência da mesma. Deve ser criada uma arquitetura de exemplo de alto nível com as informações já disponíveis para poder servir de base na continuação da implementação do roteiro. Deve haver a recolha de ativos da empresa e avaliação da sua criticidade, que irá permitir à empresa focar os seus esforços na proteção dos mesmos. Devem ser criadas políticas de segurança dos ativos para que ao serem cumpridas aumentem a sua segurança.

6.1.1 *Apresentação de caso de estudo do negócio*

Deve ser desenvolvido um caso de estudo do negócio para as necessidades exclusivas da empresa. Este deve capturar as preocupações da administração relacionadas com o mesmo, sendo que, ao mesmo tempo, se fundamenta na experiência de quem já lida com muitos dos mesmos riscos. O caso fornece o impacto comercial e a justificação financeira para a criação de um programa integrado de segurança da informação. Deve incluir informações detalhadas sobre os:

- Benefícios, incluindo maior confiabilidade e disponibilidade do sistema de controlo, da criação de um programa integrado de segurança;

- Custos potenciais priorizados e cenários de danos caso um programa de segurança de informação não seja implementado;
- Visão geral de alto nível do processo necessário para implementar, operar, monitorizar, rever, manter e melhorar o programa de segurança da informação;
- Custos e recursos necessários para desenvolver, implementar e manter o programa de segurança;

Antes de apresentar o caso de estudo do negócio à administração, deve haver um plano de negócios bem pensado e desenvolvido de implementação de segurança e plano de custos.

6.1.2 *Envolvimento e colaboração das várias entidades da empresa*

Para o sucesso do projeto devem-se garantir as capacidades mínimas de cibersegurança, este deve envolver investimentos e disponibilidade das várias áreas de atividade na empresa. A administração deve demonstrar suporte e compromisso relativamente a este projeto, uma vez que toma todas as decisões relacionadas com a empresa. É neste ponto que se deve designar um responsável de segurança ou o responsável do sector informático da empresa.

6.1.3 *Exemplo de arquitetura de alto nível*

Esta arquitetura, presente na Figura 9, é um exemplo ilustrativo, podendo ser usado numa implementação ou não, servindo assim como guia, não como uma arquitetura fixa, devendo ser adaptada às necessidades da empresa.

A Figura 9 descreve a arquitetura de alto nível para monitorizar ativos ICS, incluindo aqueles localizados em locais remotos. Enquanto um local remoto é representado, a arquitetura permite a inclusão de vários locais remotos. Isso permite uma estrutura replicável e padrão de implantação e estratégia para vários controlos de locais remotos, que podem ser adaptados às necessidades individuais do local.

A arquitetura de alto nível (Figura 9) é melhor descrita começando no sistema de controlo do local remoto. As informações neste nível aparecem como dados brutos baseados em ICS, tráfego de rede baseado em ICS ou dados de rede brutos.

As comunicações seriais são encapsuladas nos protocolos de rede. Todos esses dados são recolhidos e armazenados pelos servidores de dados do local remoto (R3).

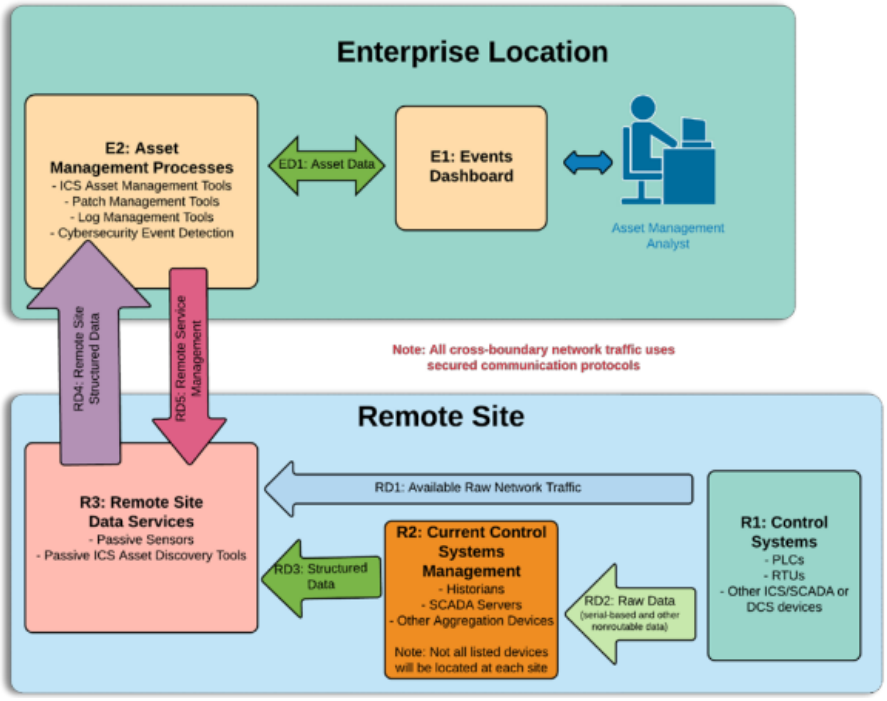


Figura 9: Arquitetura de Alto Nível [27]

Esses sensores recolhem o tráfego de rede ICS e dados brutos de rede IP dos sistemas de controlo (R1) e gestão de sistemas de controlo atuais (R2). Os dados recolhidos pelos servidores de dados do local remoto (R3) são enviados via um túnel VPN para servidores de escuta no local da empresa. Uma vez que os dados chegam do controlo do local remoto no servidor de recolha de dados empresariais, ele é ingerido nos processos de gestão de ativos (E2).

Estas ferramentas agregam os dados estruturados do local remoto (RD4) de vários locais, para criar uma visão abrangente do estado e configuração da rede. Em seguida, eventos e dados de ativos das ferramentas de gestão de processos de ativos (E2) são enviadas diretamente para o painel de eventos (E1). No painel de eventos (E1), estes são exibidos num formato fácil de ser analisado por um analista.

No caso de configuração necessária de servidores de dados de locais remotos (R3), as conexões de gestão de serviços remotos podem ser estabelecidas entre os processos de gestão de ativos (E2) e os servidores de dados do local remoto (R3). Esse tráfego é transferido pelo túnel VPN mencionado acima, sendo finalizado nos servidores de dados dos locais remotos (R3). Isso permite a configuração apenas nos servidores de dados dos locais remotos (R3), utilizando o túnel VPN estabelecido para segurança, sem permitir acesso tanto ao sistema de gestão de controlo atual (R2) ou a dispositivos de sistemas de controlo (R3).

6.1.4 *Diagrama estrutural da empresa e recolha de ativos*

Deve haver uma descrição de como é composta a empresa. Para isto deve ser realizado um diagrama de todos os cargos da empresa para se determinar os responsáveis de cada departamento e as suas funções. Deve fazer uma lista de fornecedores e parcerias com as quais a empresa tem protocolos. Dever ser feita também uma lista de dados que a empresa obtém tanto dos colaboradores como parcerias, fornecedores e clientes. Isto irá permitir observar se são recolhidos dados que não são necessários. Têm que ser identificados todos os ativos que a empresa contém, sejam estes físicos ou digitais.

Após a identificação dos ativos, devem ser identificados os mais críticos para a empresa. Estes devem ser aqueles que especialmente podem afetar a empresa em termos de negócio e na capacidade de fornecer energia ou sendo menos críticos estão mais vulneráveis a ataques.

Deve ser verificado que tecnologias de cibersegurança, protocolos e políticas de segurança já estão implementados para que estes se possam integrar na implementação do roteiro. Os ativos mais críticos serão aqueles relacionados com OT e ICS, como sensores, válvulas, o sistema de motorização destes como o SCADA, dispositivos IoT que também fazem monitorização destes dispositivos e TI, como redes de computadores, dispositivos móveis e fixos ou equipamentos de rede. Deve-se ter especial cuidado com dispositivos que façam convergência entre OT e TI, ao poderem expor os equipamentos de OT, que antes apenas estavam expostos localmente, a ataques.

6.1.5 *Identificação de criticidade de ativos e criação de políticas de segurança*

Após a obtenção dos ativos mais importantes ou críticos para a empresa, ou seja, foi feita a análise de criticidade dos ativos, devem ser analisados que riscos é que podem afetar estes ativos, qual a probabilidade de estes serem afetados, as suas vulnerabilidades, as consequências de estes serem afetados e as ameaças que podem afetá-los.

Devem-se definir, catalogar e categorizar os aplicativos e computadores sistemas dentro do ICS, bem como as redes dentro e em contacto com o ICS. O foco deve estar em sistemas em vez de apenas dispositivos, e deve incluir PLCs, DCS, SCADA e sistemas baseados em instrumentos que usam um dispositivo de monitorização, como uma HMI. Ativos que usem protocolos encaminháveis devem ser documentados.

Deve-se rever e atualizar a lista de ativos ICS anualmente e após adições ou remoções substanciais. Seguidamente deverá ser identificado um responsável pela identificação, monitorização e criação de incidentes de segurança que possam ocorrer, sendo que este deve ser o responsável de segurança.

Este irá criar uma topologia de notificação de incidentes que, posteriormente a ser aprovada pela administração, a quem irão ser informados quando for encontrado um incidente, se o incidente tem impacto numa determinada função ou quem os irá resolver. Este responsável também deverá criar uma política de segurança que, após aprovada pela administração, deverá envolver todos os colaboradores da empresa para ser eficaz. Esta deverá conter processos e procedimentos que, ao ser implementados por cada departamento, irão melhorar a postura de cibersegurança e criar boas práticas.

Esta política deve também ter em conta tanto os ativos críticos já definidos, bem como as suas prioridades. Deve ser criado um plano inicial de resposta a incidentes, onde neste estarão incluídos os incidentes que podem ocorrer mais regularmente e como responder a estes.

6.1.6 *Definir políticas e procedimentos de segurança específicos para o ICS*

Sempre que possível, as políticas e procedimentos de segurança específicos para o sector devem ser integrados nos sistemas operacionais e de gestão existente. Políticas e procedimentos ajudam a garantir que a proteção de segurança seja consistente e atual para proteger contra ameaças. Após uma análise de risco de segurança da informação ter sido realizada, o responsável de segurança deve examinar as políticas de segurança existentes para ver se elas abordam adequadamente os riscos. Se necessário, as políticas existentes devem ser revistas ou criadas políticas.

Para mais informações sobre pontos que podem ser aplicados nesta fase, pode ser consultado o documento *NIST Special Publication 1800-23 Sector Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry* [27] e *NIST Guide to Industrial Control Systems (ICS) Security* [26]. Pode também serem consultadas as normas do *NIST Framework for Improving Critical Infrastructure Cybersecurity* [28], sendo as principais para esta fase são as ID-AM, ID-BE, ID-GV, ID-RA, ID-RM e ID-SC.

6.2 FASE 2

Nesta fase o objetivo é o início da implementação do roteiro, usando os dados adquiridos na primeira fase. Deve ser criada uma arquitetura de referência usando os ativos obtidos para ter uma maior perspetiva da sua implementação. Devem ser implementados recursos e tecnologias que permitam o descobrimento, monitorização, inventariação, identificação e análise dos ativos da empresa automaticamente cada vez que estes são inseridos, permitindo que não haja falhas de segurança devido ao desconhecimento de um ativo.

Será nesta fase que começam a ser instaladas tecnologias específicas para o funcionamento e monitorização da rede elétrica como o PMI e a infraestrutura de medição avançada. Começa a centralização da recolha de registo de rede, estabelecimento de normas de segurança e criação da política de uso aceitável.

6.2.1 *Arquitetura de Referência*

Esta arquitetura de referência, é um exemplo de mais baixo nível relacionado com a Figura 9, mostrando a interligação de várias tecnologias e que deverão ser implementadas. No entanto, deve apenas servir como guia, devendo ser adaptada às necessidades da empresa, devendo coincidir com a arquitetura de alto nível desenhada pela mesma.

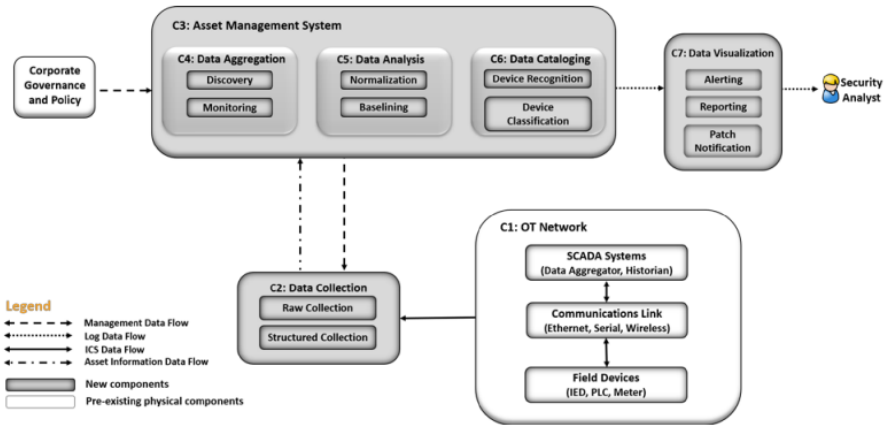


Figura 10: Arquitetura de Referência [27]

Conforme indicado na Figura 10, diferentes linhas representam diferentes tipos de dados que fluem para os vários componentes. Os dados ICS são representados com linhas sólidas. O fluxo de dados de gestão é representado com a linha a tracejado.

As informações de ativos são representadas com uma linha pontilhada com traços. Os dados de *logs* são representados com uma linha pontilhada. Cada um das formas claras representa um componente preexistente ou opcional. A rede OT consiste em dispositivos baseados em ICS, tráfego de rede ICS ou dados brutos de rede.

Outro componente que utiliza a solução ESAM é a política e governança corporativa. A governança corporativa e política podem orientar diferentes aspetos da solução ESAM, como por quanto tempo os registos serão mantidos, como classificar os dispositivos e com que frequência os relatórios são executados.A governança de cada empresa e a política será determinada pela tolerância ao risco da empresa e pelas decisões de gestão. Os componentes do projeto de referência ESAM, juntam-se para formar o ativo de sistema de gestão. Cada capacidade é descrita abaixo:

- A capacidade de recolha de dados captura os dados da rede OT no local. Os dados podem ser recolhidos na forma de captura de pacotes brutos, bem como em qualquer forma estruturada que possa vir de ferramentas ou dispositivos na rede OT. Esta capacidade pode ser configurada via canais de gestão remota, para garantir a ingestão de dados mais precisa e informada por políticas necessárias para a empresa.
- O componente de agregação de dados ingere dados da capacidade de recolha de dados e utiliza ambos os dados de descoberta e os de monitorização. A capacidade de monitorização rastreia a atividade de rede recolhida da rede OT. Após um período de treino, a capacidade de descoberta identifica novos dispositivos quando novos endereços IP e endereços MAC estão se comunicando na rede.
- A capacidade de análise de dados utiliza tanto a capacidade de normalização para trazer o tráfego de vários locais para uma única imagem e a capacidade de definir uma linha de base para estabelecer um padrão informado de como o tráfego de rede de um ativo se comporta em operações normais.
- A capacidade de catalogação de dispositivos usa simultaneamente informações dos componentes de recolha de dados. A capacidade de reconhecimento de dispositivo identifica diferentes tipos de dispositivos no sistema. Os dispositivos são identificados pelo endereço MAC para determinar o fabricante ou pela inspeção profunda do pacote para determinar o modelo, número de série ou ambos de um dispositivo se o protocolo dos ICS conter tais informações. A empresa deve verificar a conformidade com os regulamentos relevantes antes de implantar esse aspeto da solução. Em seguida, a capacidade de classificação

do dispositivo pode determinar o nível de criticidade dos dispositivos, tanto automaticamente, bem como manualmente, se solicitado.

- A capacidade de visualização de dados exibe dados dos componentes do sistema de gestão de ativos. Aqui, o recurso de alerta notifica os analistas sobre incidentes, incluindo desvios ao normal comportamento. Este componente também inclui a capacidade de gerar relatórios oportunos necessários nas operações da empresa. Uma característica chave da capacidade de criação de relatórios é a capacidade de avisar quando um *patch* de cibersegurança está disponível.

Este exemplo de implementação da arquitetura de gestão e monitorização de ativos, quando aplicado, deverá permitir à empresa detetar diferenças no comportamento normal dos seus ativos e tomar ações para prevenir disrupções.

6.2.2 *Descobrimento de ativos e monitorização*

Deve ser instalada uma plataforma ou *software* que permita o descobrimento de ativos e monitorização dos mesmos. Os objetivos ideais desta plataforma seriam permitir uma forma de descobrir os ativos passivamente, detetar ameaças a esses mesmos devido a sua monitorização e capaz de responder a incidentes em redes ICS. O comprimento destes objetivos iria permitir que os dispositivos e sistemas na empresa sejam inventariados, que seja criada uma base das operações da rede, que o tráfego de dados expectável pelos utilizadores seja estabelecido e gerido e que os eventos detetados pela plataforma fossem analisados para permitir compreender os alvos dos ataques e os seus métodos.

6.2.3 *Recolha de dados e a sua inventariação*

Deve ser instalada uma plataforma ou *sofware* que permita descobrir todos os dados necessários dos ativos e centralize essa informação para mais fácil análise e monitorização. Isto irá permitir um maior controlo dos ativos empresariais, sabendo todos os necessários para tomar uma ação sobre os mesmos se for preciso.

6.2.4 *Identificação de ativos, a sua análise e a criação de linha base*

Deve ser instalada uma plataforma ou *sofware* que permita identificar os ativos empresariais, e com essa identificação consiga reportar correções para esses mesmos ativos, que permitem atualizar o seu *firmware* e *sofware* contra vulnerabilidades, que permita receber um relatório de ameaças e vulnerabilidades que possam estar associadas aos ativos e que permita fácil visualização destes dados. Isto permite que a inteligência de ciberameaças seja recebida a partir de fontes e fóruns de partilha de informações, dando assim uma maior visão das ameaças aos ativos da empresa.

6.2.5 *Melhoria e adaptação da arquitetura de referência*

Olhando para a arquitetura de referência exemplificada na Fase 1, podem ser feitas várias adições de segurança.

Neste sentido deverão existir *firewalls* para controlo dos acessos para/da Internet e entre diferentes zonas de segurança, com regras que minimizem a interação entre camadas. Existem várias soluções no mercado específicas para o sector energético.

Estas soluções têm que permitir a segregação dos ativos de OT e TI, apenas permitir o tráfego específico para que os aparelhos OT possam funcionar, permitindo conexões seguras entre as redes de TI e OT. Se possível, ou dentro orçamento da empresa, podem ser aplicadas várias *firewalls* entre as redes OT e IT e entre a rede TI e a Internet.

Esta solução permite que cada departamento tenha a sua VLAN para que apenas os utilizadores desse departamento tenham acesso aos seus recursos e que cada aparelho de OT esteja separado por VLAN dependendo da sua função. Isto também irá permitir que outros departamentos não tenham acesso a recursos e a dados que não precisam e no caso de uma falha de segurança, esta fique contida a um departamento ou a uma zona.

Usando a *firewall* deve ser criada uma zona desmilitarizada (DMZ) onde há a separação dos conteúdos ou servidores expostos para o público e os dispositivos internos, diminuindo assim a superfície de ataque. Esta pode também ser aplicada entre os aparelhos OT e a rede IT para haver uma maior separação.

Deverá existir um IDS/IPS por forma a analisar e monitorizar os padrões de normalidade definidos, sendo que estes serão definidos quando for implementado o sistema SCADA por ser este que receberá as medições dos dados e/ou definir as

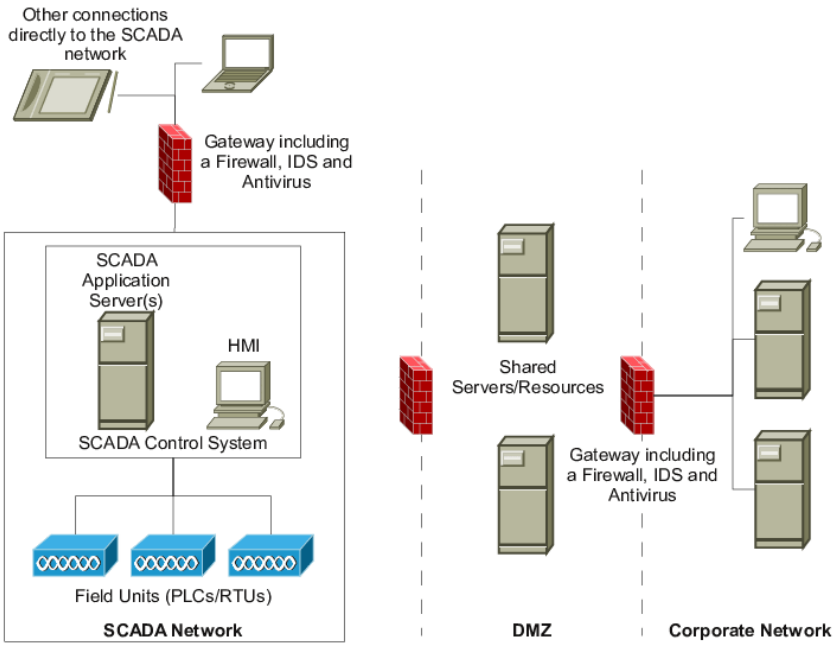


Figura 11: Exemplo de uma arquitetura com várias *firewalls* e DMZ's [26]

regras de monitorização. Existem vários IDS/IPS específicos para este sector no mercado (StationGuard by OMICRON Energy ou Graphene IDS by ICS-Security), sendo que estes devem permitir uma *deep packet inspection* (DPI) detetando assim os protocolos usados nas ligações entre dispositivos OT e detetando anomalias. Estes devem permitir ter uma visão abrangida da rede, feitos especificamente para a monitorização de redes elétricas, para uma rápida deteção de ataques para haver uma maior eficácia na resposta.

O perímetro de rede deve constituir uma primeira linha de defesa contra ameaças externas. Uma *firewall* configurada adequadamente constitui um dos fundamentais elementos de aplicação das políticas internas, fazendo a filtragem do tráfego conforme as necessidades da empresa, bloqueando tentativas de acesso exteriores não desejadas, e evitando a exposição a protocolos de comunicações desnecessários ou perigosos. Os protocolos mais comuns nas redes OT são os *Profinet*, *Profibus*, *EtherNet/IP* e *Modbus*, sendo que o uso de protocolos diferentes pode significar dados anómalos. O complemento com um sistema de IDS/IPS permite que analise o conteúdo do tráfego e detetando e/ou bloqueando padrões de ataque conhecidos.

Na Figura 11 é demonstrado um exemplo de aplicação de várias DMZ's e várias *firewalls*. Há uma aplicação de um DMZ externa que separa os servidores expostos ao público e a rede interna, tendo uma *firewall* entre a DMZ e a rede interna. Este

exemplo tem também este contexto aplicado a rede OT tendo esta também uma *firewall* entre a DMZ e a rede OT.

6.2.6 *Implementação de sistema de recolha e armazenamento do fluxo de tráfego*

A tecnologia de exportação e armazenamento do fluxo de tráfego permite recolher metadados das comunicações que atravessam um equipamento de comunicações eletrónicas, como ligações à Internet por colaboradores da empresa ou ligações ao *website* da empresa. Este sistema é crucial para identificar atividades e comportamentos maliciosos na rede ou quando se tentam ligar-lhe.

É sugerido, tanto pelo CNCS como pelo NIST, o armazenamento dos metadados de comunicações durante um período mínimo de um ano. A recolha dos metadados e comunicações deve ser efetuada no equipamento de rede ou outros equipamentos de acesso à Internet, sendo que se for necessário ter uma maior visualização podem ser recolhidos de outros equipamentos internos.

6.2.7 *Instalação de* Phasor Measurement Units

As PMUs medem sincrofasores de corrente, frequência e tensão 30 vezes por segundo, ou mais frequentemente, revelando comportamento dinâmico e transitório, como oscilações de rede eletromecânica com frequências características de décimos de Hz.

As medições de PMU são sincronizadas no tempo, geralmente por meio do sistema de posicionamento global (GPS), e podem ser alinhadas no tempo com precisão de microssegundos em extensos territórios geográficos. Isso fornece visibilidade sem precedentes das operações da rede de área ampla, estado do sistema de energia, estabilidade de tensão e condições de ilhamento, fornecendo indicações em tempo real de instabilidades da rede que podem se originar em regiões distantes. Isto leva a que este possa ajudar a evitar uma queda de energia, especialmente em empresas que tenham a sua infraestrutura elétrica mais descentralizada.

6.2.8 *Infraestrutura de medição avançada*

A Infraestrutura de medição avançada abre comunicações bidirecionais entre o utilizador de energia e o fornecedor. Isso permite decisões informadas e económicas

sobre o uso de energia e acelera a localização e a recuperação de interrupções no nível da distribuição.

Acordos de resposta de pedidos pré-arranjados com consumidores de energia permitem consumo reduzido em alimentadores de distribuição por meio de controlo dinâmico de carga durante períodos de uso de energia de pico do sistema para evitar redução de tensão de emergência. A leitura avançada de medidores (AMR) económica economiza custos operacionais. As proteções de cibersegurança estão em vigor e desenvolvidas para proteger a segurança e a privacidade desses dados.

6.2.9 *Inventariação de ativos / produção de um mapa de rede*

Após a inventariação realizada na fase anterior, esta deve ser colocada numa base de dados, *Configuration Management Database* (CMDB), para melhor visibilidade dos ativos e informações necessárias aos analistas de segurança para perceber o contexto de um alerta, a sua criticidade e impacto. Se possível deve ser adquirido *software* específico para mapear e popular a CMDB. Mas principalmente o sistema de preenchimento da base de dados deve ter:

- Adequação — O sistema deve ser aplicável para ativos OT no setor de produção de energia;
- Segurança — As conexões e o acesso ao CMDB devem ser seguros devido à sensibilidade dos dados;
- Gestão de processos — Uma ferramenta CMDB deve permitir a realização de processos de gestão de ativos;
- Descoberta automatizada de ativos — As redes ICS de uma empresa podem incluir milhares de dispositivos e, portanto, requerem automação para uma precisão e documentação rápida de ativos;
- Usabilidade — Como um sistema deve satisfazer todos os utilizadores, como proprietários de ativos, profissionais de cibersegurança e engenheiros de campo, o sistema deve ser multifuncional e permitir o uso do ponto de vista de todos os utilizadores;
- Aplicativo móvel — Um uso móvel do sistema seria benéfico para ordens de serviço relativas a determinados ativos;
- Integrações — Os utilizadores devem conseguir importar e exportar dados de/e ao sistema, se necessário;

- Suporte — Suporte a aplicativos confiáveis deve estar disponível.
- Modificabilidade — Os recursos devem ser solicitados e removíveis para/ou do sistema para ser adaptado à tarefa e ambiente;
- Facilidade de uso — Os utilizadores devem ficar satisfeitos em usar o sistema no seu trabalho;

Sendo que mesmo com um sistema adquirido é muito difícil aplicar estas funcionalidades, devem ser prioritárias as funcionalidades de adequação e segurança.

É recomendado pelo CNCS o armazenamento do endereçamento IP, versões de sistema operativo, versões de aplicações que comunicam com o exterior e dependências funcionais com outros serviços vitais. Também é importante manter atualizado um diagrama com as principais infraestruturas de comunicações de dados e os sistemas de suporte aos serviços críticos da empresa. Este permite ter uma maior perceção dos vetores de ataque à rede como desenvolver mitigações para estes.

O CNCS recomenda que no diagrama de rede deverão constar todos os segmentos de rede da empresa, endereçamento IP usado em cada um deles, endereços IP de interligação, equipamentos de interligação entre os vários segmentos e a indicação das políticas de acesso entre estes.

Tanto o controlo de ativos como o diagrama de rede devem ser atualizados regularmente, em intervalos de 6 meses ou quando há alterações significativas.

6.2.10 *Recolha centralizada de registos*

Os *logs* produzidos pelo sistema operativo e pelas aplicações de suporte à atividade são o principal instrumento de análise e investigação de um incidente de cibersegurança. Neste contexto é essencial que a empresa possua um repositório central para estes *logs* com um período mínimo de armazenamento de um ano.

Em complemento, é importante que cada servidor armazene os seus próprios *logs* por um período de um mês. A recolha centralizada de *logs* pressupõe a identificação dos principais sistemas informáticos de suporte aos serviços críticos da empresa, a configuração destes sistemas para exportar os registos e a instalação de um servidor dedicado para o seu armazenamento.

Deve ser incluída a informação de *logging* nos planos de cópias de segurança e restauro de sistemas, e realizar, se possível, as cópias de segurança em vários repositórios diferentes para aumentar a resiliência dos dados.

6.2.11 *Segurança de dados*

As informações e dados são geridos conforme a estratégia de risco da empresa para proteger a Confidencialidade, Integridade e Disponibilidade de informação (CIA). Para garantir a CIA deve-se garantir que:

- Os dados em repouso devem ser salvaguardados;
- Os dados em trânsito devem ser salvaguardados para impedir falta de integridade dos mesmos;
- Os ativos são geridos durante toda a remoção, transferências e disposição;
- Há a capacidade adequada para garantir a disponibilidade é mantida;
- As proteções contra perda e exfiltração de dados são implementados;
- Mecanismos de verificação de integridade são usados para verificar *software*, *firmware* e integridade da informação
- Os ambientes de desenvolvimento e de teste devem ser separados dos ambientes de produção;
- Mecanismos de verificação de integridade são usados para verificar a integridade do *hardware*;

Isto irá permitir um maior controlo dos dados, salvaguardando estes e mantendo a sua CIA em todos os seus estados.

6.2.12 *Criação de instrumentos de correção ou mitigação de incidentes*

Quando identificado a origem de um incidente é necessária a aplicação de medidas corretivas ou de mitigação do mesmo. Para este tipo de situações pode ser necessário, por exemplo, aplicar uma medida de mitigação para colmatar uma falha de segurança num sistema operativo ou aplicação, bloquear determinado tráfego de entrada ou de saída da empresa, corrigir uma vulnerabilidade no sítio da *internet* da empresa, ou ainda assegurar que outros sistemas ou dispositivos não foram afetados pela mesma situação ou falha.

Para isto a empresa deve ter um dos seguintes serviços, sendo este feito por terceiros ou pela empresa em si:

- Serviços de proteção contra *Distribuited Denial of Service* (DDoS);
- Mecanismos de bloqueio de tráfego para IPs e portos específicas;

- Mecanismos para identificação de IoC no parque de dispositivos da empresa;
- Se aplicável, contratos de manutenção corretiva, para todos os componentes de *hardware* e *software* presentes na CMDB;
- Se aplicável, contratos de manutenção corretiva para as aplicações pedidas pela empresa de suporte aos serviços críticos;

Os contratos de manutenção corretiva referidos anteriormente referem-se a contratos com fornecedores de *software* específico à empresa, permitindo que quando é detetada uma falha no *software*, esta possa ser corrigida o mais rápido possível.

6.2.13 *Estabelecimento de conformidade com a legislação aplicável*

A empresa deve ter sempre presente os quadros legais e regulatórios a que está sujeita. No caso de uma empresa do sector energético, considerado um serviço essencial, estão no âmbito da Diretiva SRI – Segurança das Redes e dos Sistemas de Informação e assim da Lei 46/2018 de 13 de agosto [35]. A nível mais abrangente, o Regulamento Geral de Proteção de Dados [36], que vigora desde maio de 2018, estabelece obrigações comuns a todas as empresas que efetuam tratamento de dados pessoais. A respetiva segurança é, segundo o RGPD, dependente da empresa interna da cibersegurança, de boas bases de gestão de risco e da assimilação do princípio da Segurança e Privacidade desde a conceção e por omissão.

Também se deve ter em conta o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho de 17 de abril de 2019 relativo à ENISA (Agência da União Europeia para a Cibersegurança) [37], e à certificação da cibersegurança das tecnologias da informação e comunicação, pois este apresenta várias legislações relativas a nível europeu.

Existe também a Entidade Reguladora do Sector Energético (ERSE), responsável por regular os setores do gás natural, da eletricidade e do gás de petróleo liquefeito (GPL) em todas as suas categorias em Portugal. Apesar de ser uma entidade independente, existem vários diplomas que atribuem competências regulamentares à ERSE. Os princípios que orientam a regulação da ERSE são:

- A eficiência económica na afetação dos recursos para a realização das atividades reguladas;
- A promoção da sustentabilidade económica das atividades reguladas;
- A aplicação de tarifas e preços em condições de igualdade;

- A uniformidade e a convergência tarifária, nacionalmente;
- A inexistência de subsidiares cruzadas entre atividades e entre clientes, adequando as tarifas aos custos provocados na utilização do sistema;
- A partilha justa entre empresas reguladas e clientes dos resultados alcançados nas atividades sujeitas a regulação por incentivos;
- A promoção de uma regulação económica que permita às empresas reguladas o desempenho das suas atividades de uma forma economicamente eficiente, respeitando os padrões de qualidade de serviço aplicáveis e os níveis adequados de segurança na produção, no transporte e na distribuição de energia elétrica e gás natural;

Relativamente a entidades europeias do sector energético, deve-se guiar pelo *Regulation (EU) 2019/942 of the European Parliament and of the Council of 5 June 2019 establishing a European Union Agency for the Cooperation of Energy Regulator* [38], redigido pela ACER.

6.2.14 *Estabelecimento de conformidade com normas aplicáveis à área de atividade*

À semelhança do ponto anterior, a conformidade com normas ou certificações exigidas por Lei, ou por força de exigências contratuais, ou regulatórias impostas às atividades da empresa deve ser um fator prioritário. Essa importância deve ficar organizada e patente nos instrumentos de governação interna, designadamente, no domínio da cibersegurança, na política de segurança e na metodologia de análise de risco.

O incumprimento destas normas, para além de elevar o panorama de segurança e levar a coimas, pode significar perdas de reputação ou de negócio indesejáveis e potencialmente incomportáveis.

6.2.15 *Criação de política de uso aceitável*

A Política de Uso Aceitável (PUA) de recursos de TI e OT internos é um elemento de regulação interna importante. Este documento deve delinear o uso destes recursos seguramente e seja acessível por todos os colaboradores.

É importante ter em conta que grande parte das ameaças a que se expõem as empresas diariamente estão diretamente relacionados com má utilização dos recursos

tecnológicos por parte dos colaboradores. Por isso a PUA deve abranger alguns temas como:

- Papéis e Responsabilidades;
- Manutenção dos postos de trabalho e ambiente de trabalho limpo;
- Correta utilização do endereço eletrónico para uso profissional;
- Comportamento adequado na navegação na Internet;
- A correta utilização de dispositivos móveis para uso profissional;
- Instalação e utilização de *software* aplicacional apenas necessário para exercer dos seus deveres;
- Respeito pelos princípios de ética e pela privacidade e proteção de dados;
- Administração do parque informático e do acesso aos recursos em rede; pessoais

Para que a aplicação da PUA seja o mais eficaz possível, deve ser implementado um programa de formação interno, que forneça aos colaboradores da empresa com as competências e conhecimentos adequados ao bom desempenho das suas funções e que cumpram os objetivos da PUA.

6.2.16 *Tecnologia de proteção para equipamentos de OT e IT*

Há uma variedade de tecnologias de cibersegurança que podem ser usadas para proteger sistemas de TI e OT sendo alguns exemplos:

- *Firewall*: permite filtrar o tráfego da rede, permitindo prevenir acessos não autorizados;
- IDS/IPS: Permitem detetar e prevenir ataques à rede interna da empresa;
- Antivírus: Detetam e previnem programas e ficheiros maliciosos nos dispositivos empresariais;
- Criptografia: Permite que não haja falha de integridade e da confiabilidade dos dados;
- Autenticação multifatorial: exige que os utilizadores forneçam mais de uma forma de identificação antes de poderem aceder um sistema ou rede, dificultando o acesso de utilizadores não autorizados;
- SIEM: Sistemas que recolhem e analisam *logs* e eventos de várias fontes, como *firewalls* e sistemas IDS/IPS, para identificar possíveis ameaças à segurança;

- Sistemas de gestão de *patches*: sistemas que garantem o *software* e os sistemas operativos sejam mantidos atualizados com as atualizações de segurança mais recentes, reduzindo o risco de exploração de vulnerabilidades;
- Segmentação de rede: divisão de uma rede em sub-redes menores, cada uma com os seus próprios controlos de segurança, para limitar o impacto de uma violação de segurança;
- Medidas de segurança física: sistemas de controlo de acesso, câmaras de vigilância e alarmes, para impedir o acesso físico não autorizado aos sistemas de TI e OT;

Estas tecnologias devem ser implementadas em conjunto para aumentar a cibersegurança. Algumas desta serão detalhadas no roteiro.

6.2.17 *Manutenção de dispositivos*

Manutenção e reparações de controlos industrial e componentes do sistema de informação são executados consistente com as políticas e procedimentos. Para atingir este objetivo:

- A manutenção e reparação de ativos empresariais é executada e registada, com ferramentas aprovadas e controladas;
- A manutenção remota de ativos empresariais é aprovada, registada, e realizada para prevenir acesso não autorizado;

Esta manutenção é essencial para permitir e garantir o correto funcionamento, monitorização e controlo dos ativos da empresa.

Para mais informações sobre pontos que podem ser aplicados nesta fase, pode ser consultados o documento *NIST Special Publication 1800-23 Sector Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry* por [27], *NIST Guide to Industrial Control Systems (ICS) Security* [26] , *Roadmap for Photovoltaic Cyber Security* [1], *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* por [28], *Cyber security of a power grid: State-of-the-art* [29] e ISO/IEC 27019:2017 [23]. No *Framework for Improving Critical Infrastructure Cybersecurity* [28], podem ser verificadas normas aplicadas nesta fase, sendo estas a PR-AC, PR-AT, PR-DS, PR-IP, PR-MA e PR-PT.

6.3 FASE 3

Nesta fase o objetivo será a implementação de um conjunto de técnicas e mecanismos de segurança para proteger a convergência entre os ativos de OT e IT.

Os ativos mais importantes da empresa e devem ser os primeiros a terem sido identificados e ser protegidos com a implementação de sistemas SCADA, IDS, Smart grids e SIEM.

Com a ajuda destas tecnologias, deve haver uma avaliação contínua e automatizada dos riscos e as medidas técnicas desenvolvidas para reduzir a exposição a ciberataques. As medidas de proteção operacional são projetadas para defender a rede de controlo para que, se um adversário puder obter acesso às redes de controlo, presença é detetada e ações maliciosas ou reconhecimento são dificultados.

Apesar de haver um maior controlo e maior capacidade de deteção, devem implementar-se contramedidas para aumentar a resiliência do sistema, estender o tempo e a dificuldade do ataque e minimizar o impacto no sistema caso o ataque seja bem-sucedido.

6.3.1 *Instalação de PDCs*

A instalação de PDCs permite centralizar os dados de vários PMUs e por conseguinte transmitir esses dados a várias plataformas de monitorização e/ou centralização de dados.

Isto permite a distribuição dos dados em tempo real a plataformas que precisem dos mesmos. Neste caso, o PDC servirá como um intermediário, fazendo a verificação dos dados recebidos, agregando e reencaminhando os dados para as aplicações de monitorização.

6.3.2 *Instalação do Sistema SCADA*

A instalação do sistema permite conseguir reagir rapidamente a alarmes e eventos, podendo ser vital para as operações de uma rede elétrica. Um exemplo seria o sistema SCADA notificar o operador da rede elétrica na HMI se algo não estiver a funcionar corretamente.

Se ele avaliar que o equipamento precisa ser parado, ele pode fazer isso diretamente na HMI, que envia comandos para os PLCs ou RTUs, que também enviam por meio de comandos e param o equipamento no local. Devido à notificação do sistema SCADA, o operador pode reagir rapidamente a problemas emergentes e evitar possíveis custos de manutenção.

6.3.3 *Instalação do* Energy Management System

A instalação de EMS permite reduzir os custos operacionais e melhorar a produtividade. Enquanto isso, o EMS deve atender aos requisitos de automação de equipamentos de energia e gestão de operação, para que os sistemas de gestão de energia reduzam a entrada de recursos humanos.

Permite também entender rapidamente a operação do sistema e o impacto do grau de falha de uma perspetiva global. Assim, podem ser tomadas medidas eficazmente para limitar a expansão do tamanho da falha e restaurar a operação normal do sistema.

Finalmente, o EMS permite melhorar o balanço de energia otimizando métodos e técnicas de gestão de energia e pode entender em tempo real a procura de energia e a situação de consumo das empresas que necessitam da mesma. Assim, o EMS pode efetivamente reduzir o consumo de energia e as emissões de poluentes.

Estas vantagens permitem uma maior segurança da rede, aumentando a sua monitorização para uma resposta eficaz a falhas, tanto resultantes de aspetos de falhas de componentes de OT como ciberataques.

6.3.4 *Instalação da* firewall

Devem ser instaladas *firewalls*, entre a rede ICS ou OT e a rede corporativa rede, como demonstrado anteriormente na Figura 11. Adequadamente configuradas, elas podem restringir bastante o acesso indesejado entre o sistema de controlo, computadores e controladores, melhorando assim a segurança.

Também podem potencialmente melhorar o controlo de capacidade de resposta da rede, removendo o tráfego não essencial da rede. Existem 3 tipos de *firewalls* usadas para proteção da rede ICS: *Packet Filtering Firewalls*, *Stateful Inspection Firewalls* e *Application-Proxy Gateway Firewalls*.

Packet Filtering Firewalls são as *firewalls* mais básicas, filtrando pacotes de redes pela informação mais básica. Estes fornecem um alto nível de segurança, são mais baratas que outros tipos de *firewalls* mas pode impactar o rendimento da rede e criar atrasos na mesma.

Stateful Inspection Firewalls que incorporam conhecimento adicional do modelo OSI na camada 4, filtrando pacotes na camada de rede, determinando se os pacotes de sessão são legítimos e avaliar o conteúdo de pacotes na camada de transporte. Isto permite ter um nível alto de segurança sem afetar rendimento da rede. No entanto, é uma solução cara relativamente às outras soluções apresentadas, mais complexa na implementação e pode necessitar de regras adicionais para aplicações ICS.

Application-Proxy Gateway Firewalls examina pacotes da camada de aplicação e filtra o tráfego com base em regras de aplicações específicas como, por exemplo, *browsers* ou protocolos. Isto permite ser muito eficaz na prevenção de ataques sobre os serviços de acesso remoto e configuração fornecidos pelos componentes ICS. Fornece um nível alto de segurança, mas pode impactar o rendimento da rede e criar atrasos na mesma.

A escolha de *firewalls* irá depender da capacidade financeira da empresa, as suas capacidades técnicas e as suas necessidades.

Para conjuntos gerais de regras de *firewall*, o seguinte deve ser considerado prática recomendada, mas não obrigatória:

- O conjunto básico de regras deve ser negar todas as ligações e permitir apenas as estritamente necessárias;
- As portas e serviços entre o ambiente da rede de controlo e a rede empresarial devem ser ativadas e permissões concedidas caso a caso. Deve haver uma justificação comercial documentada com análise de risco e responsável por cada entrada ou saída de fluxo de dados;
- Todas as regras de permissão devem ser específicas tanto para o endereço IP quanto da porta TCP/UDP e com informações de estado, se apropriado;
- Todas as regras devem restringir o tráfego a um endereço IP específico ou intervalo de endereços;
- O tráfego deve ser impedido de circular diretamente da rede de controlo para a rede empresarial. Todo o tráfego deve terminar na DMZ;

- Qualquer protocolo permitido entre a rede de controlo e a DMZ deve explicitamente não ser permitido entre a DMZ e as redes empresariais (e vice-versa);
- Todo o tráfego de saída da rede de controlo para a rede empresarial deve ser origem e destino restrito por serviço e porto;
- Pacotes de saída da rede de controlo ou DMZ devem ser permitidos apenas se esses tiverem um endereço IP de origem correto atribuído à rede de controlo ou aos dispositivos na DMZ;
- Dispositivos de rede de controlo não devem ter permissão para aceder à *Internet*;
- As redes de controlo não devem ser conectadas diretamente à *Internet*, mesmo que protegidas por uma *firewall*;
- Todo o tráfego de gestão de *firewall* deve ser realizado numa rede de gestão separada e segura ou numa rede com autenticação multifator. O trânsito também deve ser restrito por endereço IP a estações de gestão específicas;
- Todas as políticas de *firewall* devem ser testadas periodicamente.

Estes devem ser considerados apenas como diretrizes e recomendações. Uma avaliação cuidadosa de cada ambiente de controlo é necessária antes de implementar qualquer conjunto de regras de *firewall*.

6.3.5 *Segregação da rede*

As redes ICS e as redes empresariais podem ser segregadas para melhorar a cibersegurança usando diferentes arquiteturas. Serão apresentados dois exemplos que podem ser usados para a segregação da rede empresarial e a rede OT/ICS. Estes devem ser adaptados as necessidades e ativos da empresa.

6.3.5.1 Firewall *com uma DMZ entre a rede empresarial e a rede de controlo*

Esta arquitetura recorre a *Firewalls* com a capacidade de estabelecer uma DMZ entre as redes empresariais e de controlo. Cada DMZ contém um ou mais componentes críticos como o ponto de acesso *wireless* ou sistemas de acesso remoto e de terceiros. Com efeito, o uso de uma *firewall* compatível com uma DMZ permite a criação de uma rede intermediária.

A criação de uma DMZ exige que a *firewall* ofereça três ou mais interfaces, em vez das típicas públicas e privadas. Uma das interfaces está ligada à rede empresarial, a segunda ao controlo de rede e as restantes para os dispositivos compartilhados ou inseguros, como o servidor do historiador de dados ou pontos de acesso sem fio na rede DMZ. Implementando tráfego contínuo de entrada e saída de monitorização na DMZ é recomendado. Além disso, conjuntos de regras da *firewall* que permitem apenas conexões entre a rede de controlo e DMZ iniciados por dispositivos de rede de controlo são recomendados.

A Figura 12 fornece um exemplo dessa arquitetura.

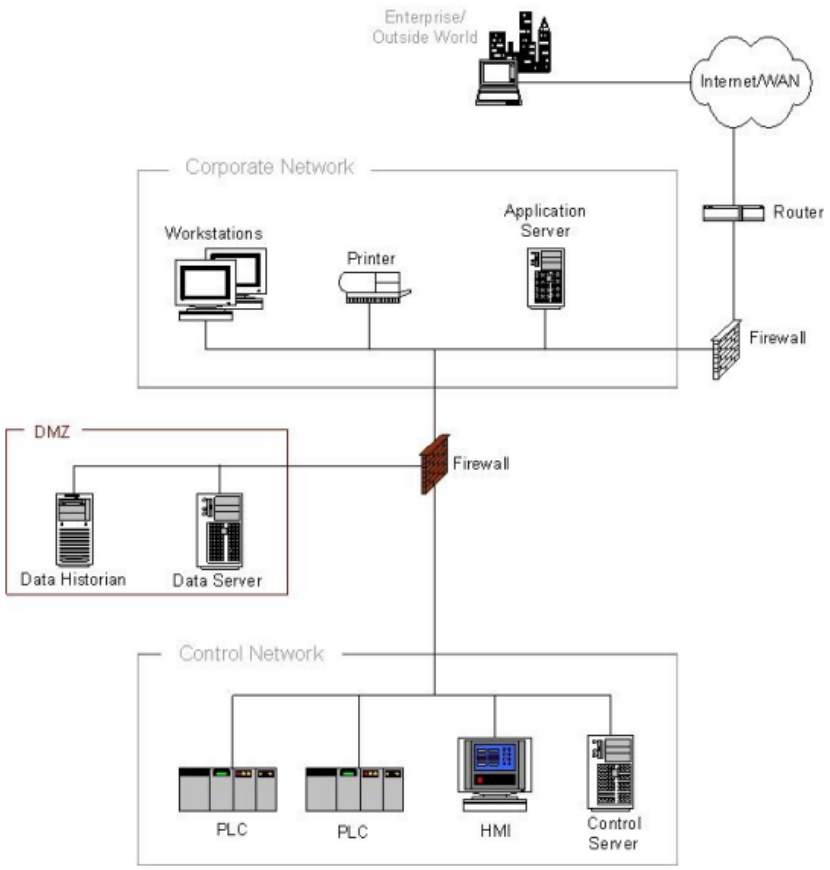


Figura 12: Exemplo de uma arquitetura com *firewall* com uma DMZ entre a rede empresarial e a rede de controlo [26]

O principal risco de segurança nesse tipo de arquitetura é que, se um computador na DMZ for comprometido, pode ser usado para lançar um ataque contra a rede de controlo via tráfego de aplicações permitido da DMZ para a rede de controlo.

Esse risco pode ser bastante reduzido se houver um esforço concentrado para endurecer e corrigir ativamente os servidores na DMZ e se o conjunto de regras da *firewall* permitir apenas conexões entre os rede de controlo e DMZ iniciadas por

dispositivos de rede de controlo. Outras preocupações com esta arquitetura são a complexidade adicional e o potencial custo aumentado de *firewalls* com várias portas.

6.3.5.2 Firewall *com pares entre a rede empresarial e a rede de controlo*

Esta arquitetura recorre a usar um par de *firewalls* posicionadas entre redes empresariais e OT/ICS, conforme mostrado na Figura 13.

Servidores comuns são situados entre as *firewalls* numa zona de rede semelhante a DMZ. A primeira *firewall* bloqueia pacotes arbitrários de prosseguir para a rede de controlo ou para a DMZ. A segunda *firewall* pode impedir que o tráfego indesejado de um servidor comprometido entre na rede de controlo e evita que o tráfego de rede de controlo impacte os servidores partilhados.

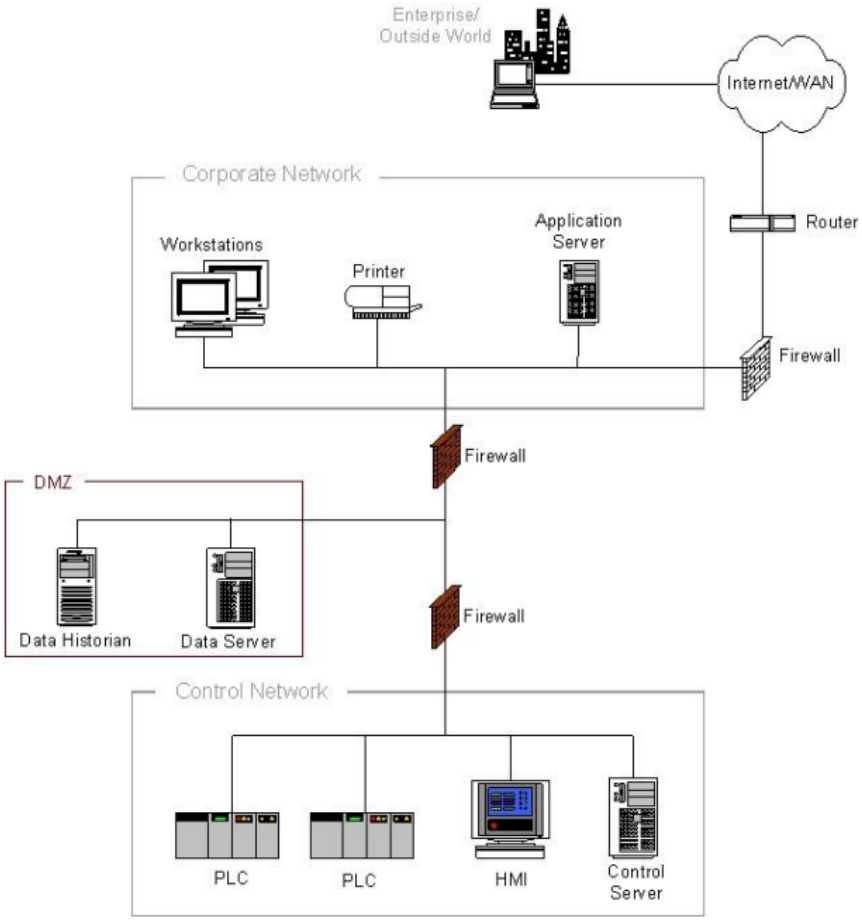


Figura 13: Exemplo de uma arquitetura com *firewalls* pares entre a rede empresarial e a rede de controlo [26]

Isto permite que o grupo de controlo e o grupo de TI tenham responsabilidades de dispositivos claramente separadas porque cada um pode gerir uma *firewall* por conta própria, se a decisão for tomada na empresa para fazê-lo. A desvantagem primária das arquiteturas de duas *firewalls* é o aumento do custo e da complexidade da gestão. Para ambientes com requisitos de segurança rigorosos ou a necessidade de uma clara separação de gestão, esta arquitetura demonstra fortes vantagens.

6.3.6 *Instalação e configuração de mecanismos de monitorização*

Esta fase prevê a instalação e configuração de um sistema de monitorização dos principais ativos de rede e sistemas de suporte às atividades da empresa. Tipicamente, um sistema de monitorização abrange a leitura regular de variáveis de sistema diretamente nos equipamentos e sistemas, como o espaço do disco, memória RAM, temperatura de componentes críticos e volume de tráfego, bem como testes à disponibilidade e bom funcionamento, incluindo tempos de resposta aceitáveis do ponto de vista dos utilizadores do serviço.

Este sistema deverá medir indicadores de disponibilidade e de qualidade dos equipamentos e serviços, despoletando alertas sempre que o valor medido ultrapasse os parâmetros normais de funcionamento.

Este sistema irá incluir o sistema SCADA (este já monitoriza os sensores de OT) e a *Smart Grid* para monitorização dos fluxos de energia da rede, sendo que estes irão despoletar alertas de segurança quando os valores esperados são diferentes.

6.3.7 *Definição de procedimentos de operação*

Esta definição significa a identificação do procedimento para a gestão de riscos, procedimentos de criação, atualização e monitorização de ativos, procedimentos de IAM, procedimentos de gestão de deteção de ameaças e vulnerabilidades, procedimentos de partilha de informações e comunicações, procedimentos de cadeia de fornecedores e gestão de entidades externas e procedimentos para a gestão de colaboradores.

Pressupõe ainda a identificação das responsabilidades e funções para os procedimentos identificados, e que informação, meios e resultados são esperados de cada procedimento, quando cada procedimento deve ser acionado, como se espera que esses mesmos procedimentos ocorram e o porquê dos mesmos.

Estes procedimentos devem ter em conta o quadro jurídico que se enquadram, como leis e normas (inter)nacionais e devem ser validados pelo departamento jurídico da empresa, se possível, ou uma entidade externa semelhante e aprovadas pela administração da empresa.

Para o procedimento para a gestão de riscos, devem ser geridos os ativos de OT e IT da empresa, incluindo *hardware* e *software*, compatível com o risco para infraestrutura crítica e objetivos empresariais.

Para o procedimento para criação, atualização e monitorização de ativos, devem ser criadas e geridas identidades para entidades que podem receber acessos lógicos ou físicos aos ativos da empresa.Devem-se controlar o acesso aos ativos da empresa, conforme o risco para infraestrutura crítica e objetivos empresariais.

Para o procedimento de IAM, devem ser estabelecidos e mantidos planos e tecnologias para detetar, identificar, analisar, gerir e responder a ameaças e vulnerabilidades de cibersegurança, conforme o risco para a infraestrutura da empresa e aos objetivos empresariais.

Para o procedimento para a gestão de deteção de ameaças e vulnerabilidades, estes devem estabelecer e manter atividades e tecnologias para recolher, analisar, alertar, apresentar e usar informações operacionais e de cibersegurança, incluindo estado e informações resumidas do outros domínios de modelo, para formar uma imagem operacional comum.

Para o procedimento da partilha de informações e comunicações, devem ser estabelecidos e mantidos planos e tecnologias para detetar, analisar e responder a eventos de cibersegurança e para suster operações durante um evento de cibersegurança.

Para o procedimento de cadeia de fornecedores e gestão de entidades externas, devem ser estabelecidos e mantidos controlos para gerir os riscos de cibersegurança associados aos serviços e ativos dependentes de entidades externas, proporcionais ao risco para infraestrutura e objetivos empresariais.

Para o procedimento para a gestão de colaboradores, devem ser estabelecidos e mantidos planos, tecnologias e controlo para criar uma cultura de cibersegurança e garantir a adequação e competência contínuas dos colaboradores, compatível com o risco para infraestrutura crítica e objetivos empresariais.

Estes devem ser revistos com alguma regularidade, para poderem ser considerados diferentes cenários e o seu constante melhoramento.

6.3.8 *Instalação e configuração de aplicações de monitorização em dispositivos*

Instalação de antivírus com visibilidade sobre todo o parque informático, ou em alternativa, no mínimo para os serviços críticos (como dispositivos OT e IoT se estes tiverem capacidade) e para os dispositivos dos administradores de sistemas, pois estes devem ser tratadas com nível máximo de criticidade por terem acesso a todos os recursos que processam e armazenam a informação da empresa. É importante permitir o controlo centralizado e que sejam aplicados automatismos para atualização regular das respetivas assinaturas, bem como agendamento de análises periódicas aos *endpoints* para deteção de infeções.

Adicionalmente deve ser criada uma política *Bring Your Own Device* (BYOD) atenta à manutenção e gestão deste tipo de dispositivos, pois estes não são controlados pela empresa e que deverá considerar, no mínimo, os seguintes aspetos:

- Armazenamento de dados da empresa em dispositivos móveis empresariais;
- Acondicionamento, circulação e eliminação de dispositivos de armazenamento móvel.

Independentemente da política de BOYD, os dispositivos móveis devem estar sujeitos a:

- Inclusão de dispositivos móveis na proteção de *endpoints*;
- Aplicação de criptografia ao conteúdo de dispositivos móveis contendo informação empresarial;

6.3.9 *Auditoria de segurança e Bases de Dados*

A existência de registos de acesso à base de dados com informação sensível ou crítica apresenta uma das medidas dissuasoras de acessos indevidos, ou ilícitos. Segundo o CNCS, o armazenamento destes registos durante um período mínimo de um ano configura um excelente instrumento para a auditoria e a análise forense em caso de incidente. Esta fase prevê a instalação e configuração de mecanismos de registo e auditoria de acesso a bases de dados com informação sensível ou crítica para a empresa.

6.3.10 *Instalação e configuração de controlo de acessos* web

Um serviço proxy age como intermediário entre o utilizador e o seu destino, adicionando estruturas e encapsulamento a sistemas distribuídos. Irá atuar no sentido de uma deteção prevenção eficaz de acessos a sistemas de comando e controlo ou repositórios de dados exfiltrados através da Internet.

Para todas as conexões remotas à estrutura da empresa deve ser usado uma VPN para encriptar todas as ligações e dados das comunicações dos funcionários.

6.3.11 *Proteção e gestão de equipamentos*

Instalação de antivírus com visibilidade sobre todo o parque informático, ou em alternativa, no mínimo para os serviços críticos e para os dispositivos dos administradores de sistemas, uma vez que as máquinas dos administradores de sistemas devem ser tratadas com nível máximo de criticidade por terem acesso a todos os recursos que processam e armazenam a informação da empresa.

É importante permitir o controlo centralizado e que sejam aplicados automatismos para atualização regular das respetivas assinaturas, bem como agendamento de análises periódicas aos *endpoints* para deteção de infeções.

Os dispositivos de comunicação e armazenamento móveis são muitas vezes esquecidos nas prioridades da cibersegurança. No entanto, trata-se já de equipamentos tidos como indispensáveis por muitas empresas e são ferramentas de trabalho que devem estar ao abrigo da política de segurança e da política de utilização aceitável de recursos TIC e, consequentemente, do Sistema Interno de Normas e Políticas.

6.3.12 Hardening *das configurações*

Este é um processo de robustecimento alinhado com um mapeamento das ameaças, das ações de mitigação dos riscos e com a execução das atividades corretivas, com foco na infraestrutura. O mesmo passa, muitas vezes, pela alteração e aplicação de restrições às configurações, quer ao nível de sistema operativo, quer aplicacional, no sentido de permitir apenas as funcionalidades e comunicações estritamente necessárias, e torná-las tão seguras quanto possível. Um processo de *hardening* pode também incluir a aplicação e manutenção regular de atualizações do *firmware*, dos

sistemas operativos e das aplicações, a revisão das permissões de acesso aos sistemas e a revisão da segurança nos acessos, entre outros.

Estas ações deverão ter maior foco nos dispositivos de OT e IoT, pois estes são os mais vulneráveis a ataques e carecem de maior atenção. Sendo que os dispositivos de OT e IoT são os que têm menos atualizações de segurança e menos segurança em geral, serão estes que terão maiores restrições nas configurações, apenas com as comunicações estritamente necessárias ao seu funcionamento que irão sempre passar pela *firewall*. Apenas os colaboradores com as permissões necessárias poderão aceder-lhes e apenas os protocolos esperados poderão fazer comunicações.

6.3.13 *Processos de deteção*

Devem ser formulados vários processos que permitem que atividade anómala seja detetada e o impacto potencial dos eventos, seja entendido. Para este fim, uma *baseline* da rede, operações e fluxos de dados esperados para utilizadores e sistemas são estabelecidos e geridos. Os eventos detetados são analisados para entender alvos e métodos de ataque, permitindo uma deteção mais rápida e diminuindo os danos que possam ser causados.

Os dados do evento são recolhidos e correlacionados de várias fontes e sensores, permitindo ter todos os dados necessários para a análise do evento de segurança. O impacto dos eventos é determinado e limites do alerta de incidente são estabelecidos, permitindo uma resposta mais concisa e rápido ao mesmo.

Devem ser criados processos para que o sistema de informação e ativos seja monitorizado para identificar eventos de cibersegurança e verificar a eficácia das medidas proteção. Isto significa que o ambiente físico é monitorizado para detetar possíveis eventos de cibersegurança, que a atividade do pessoal é monitorizada para detetar possíveis eventos de cibersegurança internos e externos, código malicioso é detetado, código móvel não autorizado é detetado, atividade de provedor de serviço externo é monitorizada para detetar potenciais eventos de cibersegurança e monitorização de pessoal, conexões, dispositivos e *software* não autorizado é executado e *scans* de vulnerabilidade são realizados.

Devem ser criados processos e procedimentos que serão mantidos e testados para garantir a deteção de eventos anormais. Estes processos serão constituídos por funções e responsabilidades para deteção são bem definidas para garantir as mesmas, as atividades de deteção estão conforme todos os requisitos aplicáveis, os

processos de deteção são testados, as informações de deteção de eventos são comunicadas as entidades com relevância e que os processos de deteção são melhorados continuamente.

6.3.14 *Instalação e configuração de um* Security Information and Event Management

Com o intuito de obter uma visão holística da segurança da informação crítica da empresa, a mesma deverá possuir um sistema de gestão e correlação de dados e eventos, conhecido como SIEM, que agrega os registos mais relevantes produzidos pelos ativos e pelas aplicações de suporte à atividade, facilitando a análise em tempo real e acelerando a tomada de ações defensivas.

Para não sobrecarregar o SIEM, sugere-se a utilização de outro repositório que funcione como repositório dos registos, para ser feita uma filtragem e normalização de dados inicial, antes dos registos serem enviados para o SIEM.

As ferramentas de SIEM permitem ajudar a reforçar a postura de segurança da empresa, incluindo:

- Uma vista centralizada de potenciais ameaças;
- Identificação e resposta a ameaças em tempo real;
- Informações avançadas sobre ameaças;
- Auditorias e relatórios de conformidade regulamentares;
- Maior transparência de monitorização de utilizadores, aplicações e dispositivos;

Segundo CNCS, o repositório e o SIEM deverão guardar os registos por um período mínimo de 1 ano e 2 anos de estatísticas.É crucial que cada ativo (por exemplo, um servidor) mantenha os seus próprios registos por um período de um mês. A recolha centralizada de registos pressupõe a identificação dos principais sistemas informáticos de suporte aos serviços críticos da empresa, a configuração destes sistemas para exportar os registos e a instalação de um serviço dedicado ao seu armazenamento.

As melhores práticas de implementação de um sistema de SIEM incluem:

- Definir os requisitos de implementação do SIEM;
- Executar testes;
- Recolher dados suficientes;

- Ter um plano de resposta a incidentes;
- Continuar a melhorar o SIEM;

Estes passos levarão a uma boa implementação do SIEM e proporcionam uma maior visibilidade da arquitetura da empresa e das suas ameaças.

6.3.15 *Automação da distribuição energética*

A automação da distribuição facilita a integração do DER, que inclui equipamentos e sistemas de nível de distribuição que podem participar ativamente das operações do sistema de energia. Exemplos são veículos elétricos de carga *plug-in* (PEV) com carregadores inteligentes e armazenamento de energia que facilita a integração de recursos de energia renovável intermitente, como eólica e solar.

Para mais informações sobre pontos que podem ser aplicados nesta fase, pode ser consultados o documento *NIST special publication 1800-23 Sector Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry* [27] *Guidelines for the selection, configuration, and use of Transport Layer Security (TLS) implementations* [39], *NIST Security and Privacy Controls for Federal Information Systems and Organizations* [40], *Roadmap for Photovoltaic Cyber Security* [1],*NIST Guide to Industrial Control Systems (ICS) Security* [26], *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* [28], ISO/IEC 27019:2017 [23], *Cyber security of a power grid: State-of-the-art* [29] e *Cybersecurity and the Smarter Grid* [15].

Há várias normas lançadas pela NIST relacionadas com esta fase, sendo estas *NIST Special Publication 800-63-3* [41], *NIST Special Publication 800-78-4* [42], *NIST Special Publication 800-70 Revision 4* [43]. No *Framework for Improving Critical Infrastructure Cybersecurity* [28], podem ser verificadas as mais relevantes para esta fase, sendo as principais as DE-AR, DE-CM e DE-DP.

6.4 FASE 4

Nesta fase, o objetivo é consolidar os conhecimentos obtidos nas fases anteriores, desenvolvendo procedimentos, normas e *standards*. Os procedimentos e normas serão o culminar do conhecimento obtidos, enquanto os *standards* serão aqueles já usados pela indústria, como o ISO 27001 e 27002 ou NIST. Deve ser também

haver uma implementação das melhores pratica usadas pela indústria para garantir a segurança.

6.4.1 *Higiene e aplicação de* patches *de cibersegurança*

Inventários, topologias de sistema, controlos ou práticas de segurança mal geridos ou não documentados podem criar vulnerabilidades que podem comprometer a segurança. Infelizmente, há pouco incentivo financeiro para administrar as melhores práticas de segurança para ICS. Essa cultura resulta em vulnerabilidades conhecidas e apresenta uma barreira significativa para a cibersegurança do DER. Existem atualmente milhares de vulnerabilidades conhecidas que existem em centenas de programas e sistemas operativos comuns.

Os inversores e outros dispositivos representam um risco significativo para o sistema de energia se não forem adequadamente *patched*. Os fornecedores de inversores e outros componentes de rede devem incorporar a capacidade de conduzir *patches* não inicializáveis para minimizar qualquer tempo de inatividade do sistema. Requisitos contratuais que definem as responsabilidades de correção para fornecedores, instaladores, agregadores e operadores de rede devem ser estabelecidos.

Além disso, regras para divulgações de vulnerabilidade também devem ser estabelecidas e formalmente documentadas. É recomendado adotar uma "Declaração de Direitos" para divulgações de vulnerabilidade que comunica o impacto e define as responsabilidades de todas as partes. Este documento deve ser aceite pela indústria para esclarecer os processos e os componentes que devem ser incluídos na divulgação, ou seja, quem descobriu a vulnerabilidade, as interfaces afetadas e o grau de risco.

6.4.2 *Criação de exercícios de segurança*

Deve haver a criação de exercícios de segurança que englobem a estrutura de TI e OT da empresa.

Deve-se testar regularmente o plano de recuperação de desastres para garantir que seja eficaz em resposta a ciberataques. O teste deve incluir simulações de diferentes cenários de ataque, incluindo ataques de *phishing* e de *ransomware*.

6.4.3 *Criação de* playbooks *para ameaças mais comuns*

Um *playbook* de resposta a incidentes é definido por um conjunto de regras que descrevem pelo menos uma ação para ser executada quando um evento ocorre. Fazem a ponte entre as políticas e procedimentos da empresa e a automatização de segurança.

- Preparação — Fase inicial em que a empresa irá preparar medidas para responder eficazmente ao incidente. Envolve um planeamento por parte das equipas, normalmente com um maior esforço do responsável de segurança ou equipa SOC, se implementada, para desenvolver mecanismos de relatórios, monitorização e notificação do incidente através dos produtos ou recorrendo a *software* adicional. Para o fazer é necessária uma compreensão adicional do produto e da forma como ele funciona.
- Deteção, Identificação e Análise — A segunda fase é a mais central e importante, ao ir determinar as ações que vão ser tomadas durante o ciclo de vida do incidente; A empresa deve detetar e validar o incidente o mais rapidamente possível, determinando a sua origem e vetores de ataque. Uma correlação com incidentes anteriores deve ser efetuada também como uma comparação das condições do incidente a um nível de segurança. É através desta análise que podemos definir a prioridade e priorização dos elementos a serem endereçados primeiro. Finalmente, quando a empresa gera o perfil do ataque, o mesmo é reportado às entidades locais, podendo prevenir ataques a outros.
- Contenção, Erradicação e Recuperação — A terceira fase foca-se em mitigar as ações do invasor. Tem dois componentes principais: interromper a propagação do ataque e evitar mais danos aos sistemas. A empresa necessita de decidir quais os métodos de contenção a empregar no início da resposta; A empresa necessita de ter uma estratégia e procedimento implementado para tomar decisões relacionadas com a contenção da ameaça que reflitam o nível de risco aceitável.
- Pós-Análise — Último passo envolve finalizar o processo de resposta a incidentes e alimentar o procedimento de melhoria de preparação e prevenção de incidentes. Primeiro, à empresa deve ter em conta as lições que aprendeu do incidente e da sua mitigação. Isto inclui documentação de quaisquer informações ou detalhes relevantes em conjunto com análise de eficácia dos procedimentos já implementados; Os dados compilados devem ser mobilizados para determinar futuros riscos. No final, a empresa necessita de dedicar planos

e recursos para retenção dos dados, incluindo partilha com entidades policiais ou partilha com parceiros;

6.4.4 *Processos de comunicação de incidentes*

Reportes de incidentes poderão ter origem de fontes externas ou existir a necessidade de comunicar para o exterior. Deverá sempre haver um ponto de contacto para informar clientes e parcerias em situações em que possam ser afetados direta ou indiretamente pelo incidente. Para os fornecedores e distribuidores, deverá ser notificado uma vez após a deteção e uma vez após a resolução do incidente. Cada uma destas notificações deverá ser feita no prazo de 48 horas desde o ocorrido e efetuado via SMS e correio eletrónico.

Para as parcerias, deverá ser enviado correio eletrónico e contacto via chamada telefónica também no prazo de 48 horas. Para além das notificações de início e de fim de incidente, estes poderão ser contactados esporadicamente para requisitar detalhes sobre o seu estado atual ou para notificar da ocorrência de eventos relevantes.

Incidentes propícios a colocar em causa a imagem da empresa perante o público devem ser reportadas de forma especial. Caso se justifique, deverá ser anunciado nas redes sociais a ocorrência do incidente, indicando, sem muitos detalhes, que estão a ser aplicadas todas as medidas necessárias para a sua resolução. No final da resolução do incidente deverá ser novamente efetuada uma publicação a indicar o seu termino.

6.4.5 *Plano de resposta a incidentes*

A empresa deve desenvolver um plano de resposta a incidentes que:

- Fornece à empresa um roteiro para implementar a sua capacidade de resposta a incidentes;
- Descreve a estrutura e empresa da capacidade de resposta a incidentes;
- Fornece uma abordagem de alto nível de como a capacidade de resposta a incidentes se encaixa na empresa na totalidade;
- Atende aos requisitos exclusivos da empresa, relacionados à missão, tamanho, estrutura e funções;
- Define quais os incidentes que deverem ser reportados;

- Fornece métricas para medir a capacidade de resposta a incidentes na empresa;
- Define os recursos e o suporte de gestão necessários para manter e amadurecer efetivamente uma capacidade de resposta a incidentes;
- É revisto e aprovado por atribuição: pessoal ou funções definidas pela empresa;
- Distribui cópias do plano de resposta a incidentes e a sua atribuição: equipa de resposta a incidentes definida pela empresa (identificada por nome e/ou função) e elementos organizacionais;
- Revê o plano de resposta a incidente: frequência definida pela empresa;
- Atualiza o plano de resposta a incidentes para abordar mudanças ou problemas organizacionais/sistema encontrados durante a implementação, execução ou teste do plano;
- Comunica as alterações do plano de resposta a incidentes: pessoal de resposta a incidentes definido pela empresa (identificado por nome e/ou função) e elementos organizacionais;
- Protege o plano de resposta a incidentes contra divulgação e modificação não autorizadas;

6.4.6 *Plano de comunicação e formação interna*

Todos os trabalhadores devem ter conhecimento do plano de reposta a incidentes. Para este fim todos os funcionários terão uma cópia física e digital do mesmo para poderem consultar sempre que necessário. Caso haja dúvidas, a equipa de resposta a incidente pode ser consultada por correio eletrónico.

Para que os funcionários se familiarizem com o plano e sobre algumas prevenções a tomar relativamente à cibersegurança, são feitas várias palestras, *webinar* ou reuniões informativas e interativas de sensibilização para discutir o plano e as ameaças mais comuns, tirar dúvidas sobre os tópicos lecionados e fazer alguns jogos interativos para os funcionários fixarem as secções mais fulcrais do plano.

Estes serão compostos por informar a estrutura do plano, perguntas sobre o mesmo, questionários e jogos interativos sobre o plano. Esta será a parte mais fulcral da formação dos funcionários, ao permitir que estes interajam com a equipa de resposta e fixem os pontos necessários para quando aconteça um incidente estes estejam preparados. Estes eventos irão decorrer a cada três meses ou quando haja

alterações significativas no plano. Este também está exposto para acesso na sala da equipa de resposta.

Adicionalmente, caso os funcionários desejem, estarão disponíveis vários questionários e jogos interativos para quem queira testar o seu conhecimento do plano. Isto dará assim dados para a equipa de resposta fazer as mudanças necessárias nas palestras e nos questionários para que o conhecimento dos funcionários do plano aumente.

Opcionalmente, quando estiver a ocorrer um incidente, poderá ser enviado uma mensagem tanto para o telemóvel como para o correio eletrónico a todos os colaboradores indicando qual o incidente ocorrido, o que pode causar o mesmo e formas de o evitar, aumentando assim a formação dos colaboradores.

6.4.7 *Criação de modelos de ameaças*

Ameaças exploram vulnerabilidades para obter informações, danificar ou manipular ativos de outras formas. Compreender a ameaça é necessário para se defender com sucesso contra ela.

A modelação de ameaças identifica ativos de alto valor, vetores de ataque e vulnerabilidades para determinar ameaças com precisão. Sistematicamente identificar e enumerar as ameaças aos sistemas de comunicação DER ajuda a direcionar o projeto de recursos de segurança apropriados para utilitários, agregadores e equipamentos de rede DER.

As vulnerabilidades devem ser descobertas, classificadas e enumeradas como parte da modelagem de ameaças processo.

Com desenvolvimento e financiamento adicional, é possível criar capacidades de previsão de ameaças que podem ser usadas para priorizar mecanismos de prevenção e proteção e implantações de sensores. Além disso, a descoberta automatizada de ameaças por meio de monitorização de rede, análise e correlação de dados é um campo de pesquisa ativo.

6.4.8 *Planos de contingência para sistemas de energia*

A funcionalidade habilitada para comunicações é incorporada no DER para permitir suporte de rede configurável, em coordenação com mercados, sistemas de controlo de concessionárias e agregadores de DER.

As comunicações também permitem aos proprietários de DER, operadores de sistemas de serviços públicos e fabricantes de equipamentos para interagir e possivelmente reconfigurar os dispositivos DER. O DER será necessário para fornecer serviços de confiabilidade crítica, como regulação de frequência e tensão.

Por muitas dessas interações ocorrerão por meio de canais de comunicação, incluindo a *internet* aberta, onde vulnerabilidades cibernéticas adicionais entram em jogo, há uma preocupação com a cibersegurança e proteção da informação. Uma questão chave é até que ponto as vulnerabilidades podem comprometer a capacidade do DER de fornecer serviços de confiabilidade crítica e resposta e recuperação do sistema.

Os operadores de rede devem considerar novos tipos de cenários de falha. Em vez de dimensionar as reservas operacionais com base nas necessidades do sistema quando o maior gerador falha, cenários de falha devem ser estudados em que as vulnerabilidades são exploradas, resultando em grandes porções da geração de eletricidade entrando *offline*.

6.4.9 *Adoção de* standards *do sector*

A implementação efetiva de práticas de cibersegurança nas empresas requer coordenação entre níveis empresariais. Os executivos determinam e comunicam a missão, as prioridades, orçamento e recursos disponíveis para o nível de negócio/processo, que os utilizam parâmetros como entradas para gerar um perfil de estrutura, uma ferramenta para estabelecer um roteiro para reduzir risco de cibersegurança.

Este é implementado no nível de operações para proteger infraestrutura crítica. Progresso relativamente ao perfil de destino e quaisquer atualizações sobre ameaças, ativos ou vulnerabilidades são comunicadas ao nível de negócios para atualizar o cenário de risco.

Operadores de rede, agregadores e fornecedores de dispositivos para o sector de energia elétrica devem empregar recomendações do *NIST 800 – 82 Guide to ICS Security* para arquitetar as redes de controlo ICS com melhor práticas, sendo estas:

- Acesso lógico controlado com *gateways* unidirecionais, DMZs, autenticação OT exclusiva mecanismos e metodologias de defesa em profundidade com múltiplas camadas de segurança;
- Restringir o acesso físico;
- Minimização de *exploits* DER por *patches* regulares, desativando portas e serviços não utilizados, adotando o princípio do menor privilégio, monitorizando auditorias já realizadas, usando programas antivírus, aplicando criptografia ou *hashes* para armazenamento de dados e comunicações, entre outros;
- Minimização da manipulação, falsificação ou falsificação de dados em trânsito;
- Empregando sistemas de deteção e prevenção de intrusão;
- Manter a funcionalidade sob pressão: componentes críticos redundantes, planos de restauração, sistemas tolerantes a falhas e degradação graciosa sem falhas em cascata, permitindo os equipamentos podem fazer a transição para operações de emergência;

6.4.10 *Plano de restauro de sistemas*

O conceito de redefinir o sistema para um bom estado conhecido ou cópias mestres não é um conceito novo, mas não é uma prática comum. A empresa devem manter cópias de todos os *softwares* para permitir a reinstalação rápida de programas usados para operações do sistema.

Usando máquinas virtuais ou *containers* permite uma reimplantação ainda mais rápida para um estado anterior seguro armazenado antes da penetração na rede. Compreender quando o sistema se tornou comprometido é essencial para selecionar a imagem correta para restaurar.

Os controlos de mudança devem ser espelhados nas cópias mestres. No entanto, permitir que as cópias mestre sejam atualizados abre vetores de ataque; proteger as imagens em bom estado é fundamental para uma recuperação eficaz.

Esta tecnologia não é usada em sistemas ICS/OT atualmente, mas pode fornecer um meio para se recuperar rapidamente de certos tipos de falhas de segurança. Encontrar a frequência certa do *software* de ponto de verificação sem degradar o desempenho da rede OT é um desafio que precisa ser resolvido para restaurar *software* para estados mais atuais.

Para mais informações sobre pontos que podem ser aplicados nesta fase, pode ser consultados o documento *Cyber security of a power grid: State-of-the-art* [29], *Cybersecurity and the Smarter Grid* [15], ISO/IEC 27019:2017 [23],*NIST Guide to Industrial Control Systems (ICS) Security* [26], *NIST Special Publication (SP) 800-40 Revision 3, Guide to Enterprise Patch Management Technologies* [44], *NIST Special Publication 800-53A* [45]. No *Framework for Improving Critical Infrastructure Cybersecurity* [28], podem ser verificadas as normas mais relevantes para esta fase, sendo as principais a RS-RP, RS-CO, RS-AN, RS-MI, RS-IM, RC-RP, RC-IM e RC-CO.

6.5 FASE 5

Nesta fase, o objetivo é a implementação de conceitos para empresas com mais capacidades, como a criação e desenvolvimento de um SOC, permitindo uma maior capacidade de monitorização e resposta da empresa. Para além de permitirem uma maior capacidade, ajudam a melhorar os seus procedimentos e aumentar a comunicação de falhas de cibersegurança dentro e fora da empresa.

É nesta fase que poderá haver partilha de informação de ameaças entre a empresa e as agências governamentais, como o CNCS para que esta esteja mais preparada caso haja ameaças já conhecidas.

Esta partilha também poderá ser feita entre as empresas do sector para que estas ameaças sejam menos eficazes. Devem também ser identificadas todas as dependências externas que sejam geridas por terceiros, pois estas podem ser um ponto de ataques por não serem geridas diretamente pela empresa.

6.5.1 *Instalação de WAMS*

A empresa, caso tenha as capacidades ou infraestrutura para poder aplicar esta solução, pode proceder à instalação do WAMS. Este sistema está destinado a empresas com maiores instalações, ou com mais locais remotos que necessitem de um maior controlo e monitorização.

A instalação deste sistema permite ter um maior nível de observabilidade do sistema de energia, deteção antecipada de oscilações no sistema de energia, sendo que permite descobrir rapidamente a localização e magnitude da oscilação, o seu

impacto no sistema local e uma estimativa de amortecimento de oscilação em tempo real.

Permite também ter capacidade de monitorização em tempo real dos locais remotos, gravando e arquivando os eventos despoletados. Isto permite prestar ajuda aos operadores quando medidas corretivas são necessárias.

6.5.2 *Instalação de um sistema de deteção de anomalias para ICS*

Se possível e dentro das capacidades da empresa, deve ser instalado um sistema de deteção de anomalias para ICS. Este *software* permite, após ter acesso a uma amostragem do que é um comportamento normal na rede da empresa, detetar anomalias e desvios do comportamento base da rede. Isto permite monitorizar a rede e detetar ameaças nesta antes de estas poderem causar consequências para a empresa e os seus ativos.

6.5.3 *Plano de continuidade de negócio*

A gestão de crise será essencial para lidar com grandes incidentes de segurança, que ponham em causa o negócio ou serviços críticos da empresa. O estabelecimento de um sistema integrado, recorrendo a um comité interno de crise formado por pessoas-chave na empresa, poupará tempo na tomada de decisões e assegurará a salvaguarda de todos os *stakeholders* internos.

Enquanto equipa de resposta a incidentes, esta deve ser uma parte importante deste sistema, mas certamente que não será o único, tendo em conta a escala que a gestão de crises tipicamente representa, em termos do âmbito de potencial ou efetivo impacto.

Há que acautelar ainda, em sede dos planos de continuidade de negócio, que esteja adequadamente refletido o papel e intervenção do sistema de gestão de crises neste âmbito.

Este plano terá que garantir que o negócio possa ser reposto o mais rápido possível, garantir a sua continuidade e repor primeiro os sectores fulcrais da empresa, como sector produtor de energia e dados guardados em servidores de *backup*.

6.5.4 *Aprovação e implementação de SOC*

Um SOC deve ter uma estrutura capaz e sustentável. Para esse efeito é necessária a aprovação, por parte da direção da empresa, de um plano de ação e orçamento para montar e operar a equipa.

Deste plano deverá constar uma proposta de enquadramento funcional na estrutura orgânica da empresa, a definição já referida da missão, da comunidade servida e portfólio de serviços, não excluindo o consequente plano de investimentos para a montagem inicial da função SOC, o plano de formação e capacitação para os recursos humanos alocados e/ou a contratar, o plano de deslocações de representação e participação nas comunidades de cibersegurança e o calendário para a sua operacionalização.

Aprovado o plano de ação, dá-se início à operacionalização do SOC. Esta ação prevê a aquisição e montagem das infraestruturas técnicas e operacionais, bem como a afetação, requalificação ou contratação dos recursos humanos necessários.

Tipicamente, um SOC precisa de um sistema de registo de ocorrências e comunicações, de canais de comunicação, de mecanismos de cifragem e de um conjunto de ferramentas de suporte à análise forense de artefactos.

Para automatizar processos, deverá ser possível a integração do sistema de ocorrências da empresa com os mecanismos de disseminação de eventos, usando uma nomenclatura comum.

Também é necessário formar os recursos humanos afetos à função SOC com as competências técnicas necessárias. Dependendo dos objetivos, as capacidades necessárias são: procedimentos de tratamento de incidentes, análise técnica de tráfego, análise técnica de artefactos e análise técnica de malware.

Uma equipa de resposta a incidentes opera sobre as notificações internas e externas que lhe chegam, donde é essencial que o SOC se dê a conhecer aos seus utilizadores, bem com às várias comunidades de cibersegurança (inter)nacionais. Para esse efeito é essencial assegurar presença regular nos principais fora de cibersegurança e participar ativamente nos seus planos de trabalhos.

6.5.5 *Auditoria de segurança*

A execução de um plano de auditorias tem o objetivo de pôr à prova os controlos de segurança implementados na empresa. O SINP, se existir, poderá ser um guião apropriado para as auditorias a efetuar, uma vez que ao seu abrigo deverão estar as políticas de segurança aplicáveis, de onde emanarão os controlos que devem ser alvo de auditoria.

Pretende-se, pois, que as auditorias visem os processos de negócio da empresa, conforme as prioridades e criticidade previamente definidas.

É aconselhável que eventuais auditorias internas sejam complementadas com auditorias externas, a cargo de empresas especializadas, e que o plano contemple, no mínimo, uma periodicidade anual para a realização de uma auditoria geral e abrangente, sem prejuízo de outras auditorias de cariz mais específico que podem ser realizadas com períodos mais frequentes, ou até mediante necessidade.

6.5.6 *Realização de melhorias*

O planeamento e os processos de recuperação são melhorados pela incorporação de lições aprendidas para atividades futuras. Isto permite que a empresa esteja sempre a fazer revisões aos seus processos para maior adaptação às ameaças existentes.

Para isto, os planos de recuperação incorporam lições aprendidas e as estratégias de recuperação são atualizadas. Estes processos devem ser revistos de 6 a 6 meses ou quando há uma alteração significativa na estrutura da empresa.

6.5.7 *Participação em exercícios de cibersegurança*

Os exercícios de cibersegurança servem dois objetivos importantes: testar as capacidades, os procedimentos para resposta a incidentes, e melhorar a articulação interna e externa com as partes interessadas.

6.5.8 *Participação externa*

A empresa entende o seu papel, dependências e dependentes no ecossistema maior e contribui para a comunidade mais ampla compreensão dos riscos. Ele recebe, gera

e revê informações prioritárias que informa a análise contínua dos seus riscos à medida que os cenários de ameaças e tecnologias evoluem.

A empresa compartilha essas informações interna e externamente com outros colaboradores. A empresa usa informações em tempo real ou quase em tempo real para entender e agir consistentemente sobre os riscos cibernéticos da cadeia de fornecedores associados aos produtos e serviços que presta e que utiliza.

Além disso, ele comunica-se proativamente, usando mecanismos formais e informais para desenvolver e manter uma forte oferta relacionamentos em cadeia.

6.5.9 *Protocolos de colaboração*

Deve ser feito um protocolo de colaboração com o CNCS para que esta possa auxiliar na implementação das medidas de cibersegurança e ser informado caso ataques ou quebras de segurança aconteçam.

Devem ser também feitos, se possível, protocolos de colaboração entre empresas de sector energético e associações sectoriais para poderem ser partilhadas informações relacionadas com falhas de cibersegurança para poderem ser realizadas contramedidas para ataques relacionados com a informação obtida.

O responsável de segurança e/ou o SOC ficarão como ponto de contacto entre o CNCS, outras empresas do sector e a empresa. Para manter este contacto devem ser criados canais de comunicação entre a empresa e o CNCS, e entre a empresa e empresas do sector que tenham protocolos.

Estes canais devem ser seguros e cifrados para que a informação transmitida por estes não seja comprometida.

Para mais informações sobre pontos que podem ser aplicados nesta fase, pode ser consultados o documento *Roadmap for Photovoltaic Cyber Security* [1], *NIST Guide to Industrial Control Systems (ICS) Security* [26] e *Framework for Improving Critical Infrastructure Cybersecurity* [28].

7

CONCLUSÕES

Ao realizar este projeto, foi concluído que apesar de já haver *standards*, normas e pontos gerais para aumentar cibersegurança no setor energético, este não tinha um caminho específico para implementar a segurança. Para isto foi preciso realizar pesquisas para centralizar essa informação. Foram descobertas tecnologias que desconhecia, relacionadas com a cibersegurança. Cada sector tem tecnologias específicas e o sector energético tens as suas em que permite a monitorização e proteção dos seus ativos como os sistemas SCADA, WAMS ou o uso de *smart grids*.

Apesar de saber que é um sector crítico para a sociedade, não tinha a perspetiva dos ataques já realizados e as suas consequências, sendo que ao realizar este trabalho pude expandir o meu conhecimento relativamente a este aspeto. O projeto permitiu-me, para além de, rever conceitos que já sabia relacionados com cibersegurança e descobrir novos.

Sendo que é um setor em que é realizada produção, neste caso de energia elétrica, significa que muitas das peças para gerir uma rede industrial também se enquadram neste, sendo a peça principal as tecnologias operacionais, sendo composta, por exemplo, por sensores, medidores ou válvulas.

Estas tecnologias têm que trabalhar com IT criando pontos de vulnerabilidade, sendo um dos objetivos deste roteiro reduzir estas. Também foi preciso ver que leis, normas e *standards* são usados pelo sector, pois estes têm que ser seguidos para criar a maior segurança.

O maior desafio foi a redação do roteiro de capacidades mínimas, de colocar as peças no sítio certo para que fizessem sentido cronologicamente na implementação deste, pois apesar de ter os dados suficientes para a redação do mesmo, não existe ainda um roteiro do sector com uma estrutura fixa para servir de guia. Tendo efetuado estas pesquisas, aprendi muito como o setor funciona e o paradigma específico do mesmo.

O resultado de todas as pesquisas realizadas foi a redação do roteiro de capacidades mínimas de cibersegurança no sector energético. Para além da redação do roteiro, este documento representa uma aglomeração de vários conhecimentos relativamente

ao sector energético e industrial em termos de cibersegurança, podendo este ser usado para aumentar o entendimento das IT e OT.

Para trabalho futuro, o mais importante seria testar o roteiro numa empresa do mercado e poderiam ser feitos vários capítulos mais específicos para cada área do sector, pois, apesar de cada área ser composta pelos mesmos componentes, cada uma tem a sua especificidade. Seria também importante aprofundar mais as capacidades deste roteiro por ser uma área bastante complexa e com vasta informação.

BIBLIOGRAFIA

[1] J. Johnson, *Roadmap for Photovoltaic Cyber Security*, 2017. URL: https://sunspec.org/wp-content/uploads/2020/01/Roadmap-for-Photovoltaic-Cyber-Security-SAND2017-13262-4-10-2018.pdf.

[2] E. Vincent e C. Pietralunga, *Cyberattacks on the rise in Europe amidst the war in Ukraine*, 2023. URL: https://www.lemonde.fr/en/europe/article/2023/04/03/the-rise-of-cyberattacks-in-europe-amidst-the-war-in-ukraine_6021493_143.html.

[3] B. Kite, *The 2021 ransomware risk pulse: Energy sector*, 2022. URL: https://blackkite.com/whitepaper/the-2021-ransomware-risk-pulse-energy-sector/.

[4] L. Bellucci, *Sector primer series: Energy*, 2019. URL: https://www.spglobal.com/spdji/en/documents/education/education-sector-primer-series-consumer-staples.pdf.

[5] L. Kaspersky, *What is Cyber Security?*, 2023. URL: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

[6] F. Habte, *What is network security? the different types of protections*, 2022. URL: https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/.

[7] S. Rose, O. Borchert, S. Mitchell e S. Connelly, «Zero Trust Architecture», rel. téc., ago. de 2020. DOI: 10.6028/nist.sp.800-207.

[8] M. Curphey e R. Arawo, «Web application security assessment tools», *IEEE Security & Privacy*, vol. 4, n.º 4, pp. 32–41, 2006. DOI: 10.1109/MSP.2006.108.

[9] R. Odierno, *Operations security (OPSEC) - federation of American scientists*, 2014. URL: https://irp.fas.org/doddir/army/ar530-1-2005.pdf.

[10] P. Fallara, «Disaster recovery planning», *IEEE Potentials*, vol. 23, n.º 5, pp. 42–44, 2004. DOI: 10.1109/MP.2004.1301248.

[11] Microsoft Security, *What is SIEM?*, 2023. URL: https://www.microsoft.com/pt-pt/security/business/security-101/what-is-siem.

[12] P. Endesa, *O Que São as smart grids?*, set. de 2021. URL: https://www.endesa.pt/particulares/news-endesa/inova%C3%A7%C3%A3o/o-que-sao-smart-grids.

[13] C. Wangsness, *What is a SCADA system and how does it work?*, 2022. URL: https://www.onlogic.com/company/io-hub/what-is-a-scada-system-and-how-does-it-work/.

[14] T. Babnik, K. Görner e B. Mahkovec, «Wide Area Monitoring System», *Monitoring, Control and Protection of Interconnected Power Systems*, pp. 65–82, 2014. DOI: 10.1007/978-3-642-53848-3_5.

[15] C. Hawk e A. Kaushiva, «Cybersecurity and the Smarter Grid», *The Electricity Journal*, vol. 27, n.º 8, pp. 84–95, 2014, ISSN: 1040-6190. DOI: https://doi.org/10.1016/j.tej.2014.08.008. URL: https://www.sciencedirect.com/science/article/pii/S1040619014001791.

[16] T. Inc, *What is Operational Technology (OT)?*, 2023. URL: https://www.tenable.com/principles/operational-technology-principles.

[17] United Nations, *Group of governmental experts on developments in the field of information and telecommunications in the context of international security*, 2015. URL: https://digitallibrary.un.org/record/799853.

[18] The Hague Program, *Cumulative recommendations in the UN GGE Reports*, 2015. URL: https://www.thehaguecybernorms.nl/cumulative-recommendations-in-the-un-gge-reports.

[19] I. Berger, *ISO 9001:2015 - Versão Final publicada*, set. de 2015. URL: https://www.sgs.pt/pt-pt/news/2015/09/publicacao-iso-9001.

[20] S. Portugal, *Saúde & Segurança ISO 14001 – Sistema de Gestão Ambiental*, 2013. URL: https://www.sgs.pt/pt-pt/health-safety/quality-health-safety-and-environment/environment/environmental-assessment-and-management/iso-14001-2015-environmental-management-systems.

[21] A. Portugal, *ISO 50001*, 2023. URL: https://apcergroup.com/pt/certificacao/pesquisa-de-normas/188/iso-50001.

[22] S. Portugal, *ISO 45001: Sistemas de Gestão de Saúde e Segurança Ocupacionais*, 2018. URL: https://www.sgs.pt/pt-pt/sustainability/social-sustainability/audit-certification-and-verification/iso-45001-occupational-health-and-safety-management-systems-ohsms.

[23] Ago. de 2019. URL: https://www.iso.org/standard/68091.html.

[24] CNCS – Centro Nacional de Cibersegurança, *Roteiro para Capacidades Mínimas de Cibersegurança*, 2019. URL: https://www.cncs.gov.pt/docs/cncs-roteiro-capacidades-minimas-ciberseguranca.pdf.

[25] A. Marques e L. Santos, *CNCS - Centro Nacional de Cibersegurança*, 2020. URL: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf.

[26] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams e A. Hahn, «Guide to Industrial Control Systems (ICS) Security», rel. téc., jun. de 2015. DOI: 10.6028/nist.sp.800-82r2.

[27] J. McCarthy, L. Acierto, J. Kuruvilla et al., *Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry*, en, 2020-05-19 de 2020. DOI: https://doi.org/10.6028/NIST.SP.1800-23.

[28] «Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1», rel. téc., abr. de 2018. DOI: 10.6028/nist.cswp.04162018.

[29] C.-C. Sun, A. Hahn e C.-C. Liu, «Cyber security of a power grid: State-of-the-art», *International Journal of Electrical Power e Energy Systems*, vol. 99, pp. 45–56, 2018, ISSN: 0142-0615. DOI: https://doi.org/10.1016/j.ijepes.2017.12.020. URL: https://www.sciencedirect.com/science/article/pii/S0142061517328946.

[30] R. S. de Carvalho e D. Saleem, «Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources», em *2019 Resilience Week (RWS)*, vol. 1, nov. de 2019, pp. 226–231. DOI: 10.1109/RWS47064.2019.8972000.

[31] S. Dong, J. Cao e Z. Fan, «A Review on Cybersecurity in Smart Local Energy Systems: Requirements, Challenges, and Standards», *CoRR*, vol. abs/2108.08089, 2021. arXiv: 2108.08089. URL: https://arxiv.org/abs/2108.08089.

[32] P. Hu, B. Yang, D. Wang et al., «Research on Cybersecurity Strategy and Key Technology of the Wind Farms' Industrial Control System», em *2021 IEEE International Conference on Electrical Engineering and Mechatronics Technology (ICEEMT)*, jul. de 2021, pp. 357–361. DOI: 10.1109/ICEEMT52412.2021.9601591.

[33] U. Department of Energy, *Operational Technology Cybersecurity for Energy Systems*, 2022. URL: https://www.energy.gov/femp/operational-technology-cybersecurity-energy-systems#whyot.

[34] IEA, *Portugal 2021*, 2021. URL: https://www.iea.org/reports/portugal-2021.

[35] *Lei n.º 46/2018, de 13 de Agosto*. URL: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2930%5C&tabela=leis%5C&ficha=1%5C&pagina=1.

[36] *Regulamento Geral sobre a Proteção de Dados*, en. URL: https://eur-lex.europa.eu/PT/legal-content/summary/general-data-protection-regulation-gdpr.html.

[37] European Parliament, *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, 2019. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

[38] European Parliament, *Regulation (EU) 2019/942 of the European Parliament and of the Council of 5 June 2019 establishing a European Union Agency for the Cooperation of Energy Regulators*, jun. de 2019. URL: https://eur-lex.europa.eu/eli/reg/2019/942/oj.

[39] K. A. McKay e D. A. Cooper, «Guidelines for the selection, configuration, and use of Transport Layer Security (TLS) implementations», rel. téc., ago. de 2019. DOI: 10.6028/nist.sp.800-52r2.

[40] National Institute of Standards and Technology, «Security and Privacy Controls for Federal Information Systems and Organizations», rel. téc., abr. de 2013. DOI: 10.6028/nist.sp.800-53r4.

[41] P. A. Grassi, M. E. Garcia e J. L. Fenton, «Digital identity guidelines: revision 3», rel. téc., jun. de 2017. DOI: 10.6028/nist.sp.800-63-3.

[42] W. T. Polk, D. F. Dodson, W. Burr, S. Francomacaro e D. A. Cooper, «Cryptographic Algorithms and Key Sizes for Personal Identity Verification», rel. téc., mai. de 2015. DOI: 10.6028/nist.sp.800-78-4.

[43] S. D. Quinn, M. Souppaya, M. Cook e K. Scarfone, «National checklist program for IT products - guidelines for checklist users and developers», rel. téc., fev. de 2018. DOI: 10.6028/nist.sp.800-70r4.

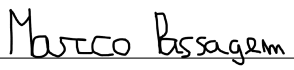
[44] M. Souppaya e K. Scarfone, «Guide to Enterprise Patch Management Technologies», rel. téc., jul. de 2013. DOI: 10.6028/nist.sp.800-40r3.

[45] National Institute of Standards and Technology, «Assessing security and privacy controls in information systems and organizations», rel. téc., jan. de 2022. DOI: 10.6028/nist.sp.800-53ar5.

D E C L A R A Ç Ã O

Declaro, sob compromisso de honra, que o trabalho apresentado neste projeto, com o título *Roteiro de capacidades mínimas de cibersegurança no sector energético*, é original e foi realizado por Marco António Vitorino Passagem (2210256) sob orientação de Professor Ricardo Jorge Pereira Gomes (ricardo.p.gomes@ipleiria.pt).

Leiria, Setembro de 2023



Marco António Vitorino Passagem