Profissionais do Futuro

Cibersegurança e Ética de Dados no Setor Elétrico

Guia de conteúdo para docentes

Publicado por
Profissionais do Futuro: Competências para a Economia Verde

Ministério da Educação (MEC)

Ministro
Camilo Santana

Secretário de Educação Profissional e Tecnológica
Getúlio Marques

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Diretor Nacional
Michael Rosenauer

Diretor de Energias Renováveis e Eficiência Energética
Johannes Kissel

Diretora do Projeto Profissionais do Futuro
Julia Giebeler Santos

Coordenação e revisão técnica da publicação
Caroline Luciane Broering Dutra – GIZ
Roberta Hessmann Knopki – GIZ

Autor
Rodrigo Antonio Sbardeloto Kraemer
Marcos Izumida (coordenação geral dos autores)

Revisão e edição de texto
Ismael Danilo Lima Freitas – GIZ
Luis Felipe Jaber – GIZ

Coordenação da diagramação
Lucas Tolentino – GIZ

Projeto gráfico e diagramação
João Bosco Gouvea Ramos

Brasil, janeiro de 2023

Por meio da:

Sumário

Abertura

Com a digitalização do setor elétrico, as infraestruturas de operação estão cada vez mais absorvendo tecnologias dos sistemas de TI, e, junto disso, vêm os desafios de proporcionar um ambiente seguro e confiável.

É evidente o crescente número de ataques cibernéticos que vem ocorrendo no mundo. Empresas têm arcado com prejuízos significativos em decorrência de vazamentos de dados sensíveis, roubos e manipulações de dados e até mesmo danos físicos às infraestruturas efetuados por cibercriminosos. Consequentemente, as preocupações com relação a estes tipos de ataques têm estimulado o investimento das empresas em cibersegurança. Porém, pesquisas mostram que, na média, estes investimentos ainda não são suficientes [1].

Diante deste contexto, a falta de investimento em cibersegurança pode ser vital se tratando de infraestruturas críticas, como é o caso do setor elétrico, já que inúmeros setores da economia dependem de energia para a continuidade de seus negócios.

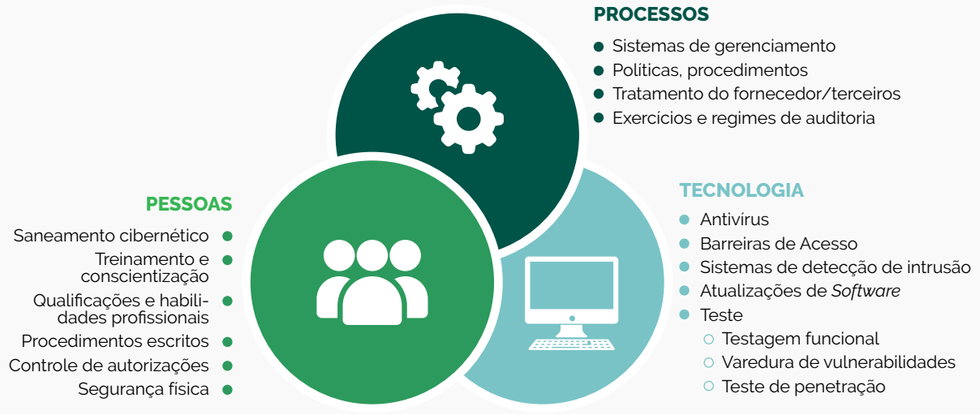
Nas últimas décadas, o setor elétrico passou por grandes mudanças devido ao desenvolvimento de novas tecnologias e padrões internacionais, principalmente buscando o desenvolvimento do setor de uma forma mais limpa e sustentável. Isso contribuiu para uma integração entre dispositivos de diferentes fabricantes uma vez que os protocolos de comunicação não eram compatíveis entre si, por exemplo. Ainda, a integração de novos dispositivos e sistemas como *smart meters*, infraestruturas inteligentes de recarga de veículos elétricos, dispositivos de microrredes, entre outros, geram uma quantidade consideravelmente maior de informações, muitas das vezes sensíveis, que devem ser tratadas e armazenadas conforme legislação de proteção de dados vigente. Dessa forma, tanto a infraestrutura operacional quanto a infraestrutura administrativa de uma organização podem estar em um mesmo sistema, e este sistema estar exposto à internet. Neste sentido, muitas das vulnerabilidades e ameaças que antes preocupavam apenas às equipes de TI, agora também devem ser consideradas pelas equipes de operação e manutenção.

Muito se desenvolveu em termos de equipamentos, *softwares* e padrões para cibersegurança em ambientes industriais desde então. Porém...

> *"Se você acha que a tecnologia pode resolver seus problemas de segurança, então você não entende nem de segurança nem de tecnologia."*
>
> *Bruce Schneier, 2015*

Essa citação demonstra bem quão importante é a implementação da cultura de cibersegurança nas organizações. Muito se fala em dispositivos de segurança e equipes de cibersegurança qualificadas, mas pouco se leva em consideração o fator humano em ataques cibernéticos [2]. Atualmente, a maioria dos ataques se utilizam de estratégias de engenharia social para conseguir o acesso a credenciais e a senhas de um sistema. Ao decorrer desta disciplina, ficará claro que as ações para a redução de riscos de segurança não dependem apenas de dispositivos ou *softwares* eficazes, mas sim de um conjunto de ações, incluindo a informação e a educação das pessoas envolvidas no processo da empresa.

Figura 1. Contramedidas para os riscos de cibersegurança.[1]



Nesse contexto, esse e-book traz conteúdos relevantes aos/às docentes de disciplinas sobre cibersegurança no setor elétrico e consiste em apresentar, inicialmente, conceitos e termos de cibersegurança, além do contexto em que se encontra o setor elétrico diante destes riscos, de forma a nivelar os/as alunos/as. Posteriormente, serão apresentadas as regulamentações vigentes relativas à proteção de dados de forma geral e específicas para o setor elétrico. Ainda, técnicas para avaliação e reconhecimento de riscos serão abordadas para que seja possível implementar estratégias para mitigação destes riscos. Este documento traz os insumos para que o/a docente complemente e aprofunde cada tópico da maneira que melhor se adaptar a seu/sua curso/disciplina.

1. Fonte: https://www.dnv.com/expert-story/maritime-impact/Cybersecurity-given-priority-in-TSMA3.html

Objetivos

É evidente a necessidade de abordar o tema cibersegurança nas indústrias quando analisamos os prejuízos causados por ataques cibernéticos, principalmente quando estamos discutindo sobre a segurança de infraestruturas críticas como é o caso do setor elétrico. Portanto, este e-book tem como finalidade auxiliar e orientar o/a professor/a acerca dos conteúdos relacionados à cibersegurança no setor elétrico. Os conteúdos deste e-book são apresentados, distribuídos nos seguintes objetivos de aprendizagem a serem alcançados junto aos/às alunos/as:

- **Abordar conceitos e termos principais relacionados à cibersegurança:** reforçar os conceitos para discentes com ou sem conhecimento prévio do tema. Pode ser entendido como uma etapa de nivelamento.

- **Expor os desafios atuais do setor elétrico com relação à cibersegurança:** apresentar a evolução tecnológica do setor elétrico para que, dessa forma, os/as alunos/as consigam entender melhor os desafios atuais de cibersegurança deste setor.

- **Abordar os protocolos de comunicação e sistemas utilizados no setor elétrico:** grande parte dos pontos de vulnerabilidade em uma infraestrutura de operação se origina em virtude dos protocolos de comunicação e sistemas de gerenciamento. Dessa forma, entender esses pontos auxilia a compreensão sobre onde aplicar as estratégias de mitigação de riscos.

- **Abordar as proteções contra *malware*:** possibilitar aos/às alunos/as o entendimento de que as proteções contra ataques cibernéticos vão muito além de *softwares* e equipamentos: envolvem pessoas e políticas educacionais.

- **Apresentar técnicas de identificação e avaliação de riscos:** permitir aos/às discentes vislumbrar as possibilidades disponíveis na literatura acerca das metodologias e normas utilizadas para identificação de riscos e, com isso, possibilitar a aplicação de ações de redução dos riscos constatados.

- **Apresentar regulamentações e normas relacionadas à proteção de dados:** abordar não apenas as leis para proteção de dados válidas para todos os setores da indústria, como é o caso da Lei Geral de Proteção de Dados (LGPD), mas também as normas específicas do setor elétrico e como elas se complementam.

- **Abordar os aspectos éticos do uso e manipulação de dados:** não basta o cumprimento dos requisitos mínimos das regulamentações, é necessário apresentar aos/às estudantes a importância de se promover um ambiente de ética no processamento de dados sensíveis e os impactos causados pelas más condutas neste sentido.

- **Apresentar ações para melhoria da segurança de infraestruturas:** expor aos/às alunos/as as estratégias utilizadas em infraestruturas de operação em termos de melhorias físicas e ao mesmo tempo abordar modelos de gerenciamento de riscos para demonstrar a eficiência da ação conjunta destas duas estratégias.

- **Apresentar ações para redução de risco de cibersegurança:** abordar os diferentes tipos de ataques que podem ocorrer, não apenas em ambiente virtual, mas também físico, expondo a importância da aplicação de um conjunto de ações para combate a ataques cibernéticos.

- **Apresentar técnicas para preservar a integridade dos dados:** abordar os processos geralmente utilizados neste sentido a fim de diferenciar proteção de dados de integridade de dados e o que isso impacta nos processos de uma organização do setor elétrico.

Capítulo 1: Análise e aplicação dos principais conceitos de cibersegurança

Nota para o/a professor/a – Ao mesmo tempo que este capítulo servirá como base teórica para os/as alunos/as, apresentará uma visão atual do setor elétrico diante de regulamentações sobre cibersegurança e as principais vulnerabilidades enfrentados pela indústria. Essa visão sistêmica aliada aos conceitos básicos proporcionará uma visão crítica aos/às discentes no decorrer da disciplina, de modo a estimular debates acerca do tema.

1.1. Conceitos de cibersegurança e de vulnerabilidade

O desenvolvimento da tecnologia, além de trazer consigo muitas facilidades e inúmeras novas oportunidades de negócios, também oferece riscos. Atualmente qualquer setor da sociedade, seja ele público ou privado, está conectado de alguma forma à internet e, com isso, exposto à possibilidade de ataques cibernéticos. Um relatório recente da empresa NSFOCUS coloca o Brasil em nono lugar na lista dos países mais atuantes em cibercrimes no mundo [3], sendo que a maioria dos ataques originados no Brasil são destinados aos próprios brasileiros, na forma de ataques do tipo *phishing* e DDoS (do inglês, *Distributed Denial of Service*).

Saiba Mais: Apesar do crescente número de ciberataques e dos consideráveis prejuízos, as empresas em geral não destinam investimento necessário para se adequarem à nova realidade e se manterem protegidas.
https://www1.folha.uol.com.br/seminariosfolha/2021/07/ciberseguranca-e-vista-como-prioridade-em-empresas-mas-falta-investimento.shtml

É possível observar que com o avanço da tecnologia e de ataques cibernéticos, também há o surgimento de novos termos como *phishing* e DDoS. Portanto, antes de adentrarmos em uma análise sistemática do estado atual do setor elétrico na cibersegurança ou abordarmos meios de prevenirmos possíveis ataques, faz-se necessário expor algumas definições e termos importantes.

Se tratando de cibersegurança, podemos definir um **RISCO** como sendo a probabilidade de uma **AMEAÇA** ser concretizada diante das **VULNERABILIDADES** existentes nos **ATIVOS** de uma empresa. Veja a Figura 2.

Ameaças são ações ou elementos que podem causar dano a um ativo. *Malwares*, que são programas de computadores inseridos em um sistema de forma disfarçada e desenvolvidos para executar alguma tarefa específica, são um exemplo de ameaça. A Figura 3 apresenta alguns tipos de *malwares* mais conhecidos e utilizados atualmente.

Já uma vulnerabilidade pode ser considerada como o "elo mais fraco" de uma infraestrutura ou de um sistema. Alguns exemplos de vulnerabilidades que podem ser citadas, são:

Software: é comum o usuário, ao instalar um programa de computador, ter de aceitar os termos de uso ou Contrato de Licença de Usuário Final (em inglês, *End-User License Agreement* – EULA) antes de utilizar o *software* de fato. Isso ocorre pois, uma vez que os *softwares* são desenvolvidos por pessoas, são passíveis de conter erros, e essa é uma maneira das empresas se protegerem destes erros. Por exemplo, é normal que empresas disponibilizem pacotes de atualizações dos programas para correção de erros encontrados após períodos de utilização do usuário.

Hardware: equipamentos antigos que não possuem mais suporte para novas atualizações de *firmware* ou equipamentos atuais que não são atualizados com frequência acabam por apresentar vulnerabilidades, muitas das vezes conhecidas.

Firmware: é um tipo de *software* desenvolvido especialmente para *hardwares*, também conhecido como "*software* embarcado". Estes programas são um conjunto de instruções operacionais que fazem os *hardwares* funcionarem e são programados diretamente no equipamento de destino. A falta de atualização destes *firmwares* é um tipo de vulnerabilidade, pois permite que cibercriminosos explorem algum defeito conhecido.

Engenharia Social: essa técnica tem como foco usuários descuidados ou desinformados que estão suscetíveis a abrir e-mails ou ativar programas de origem duvidosa de forma a roubar dados confidenciais, infectar um dispositivo com algum *malware* etc.

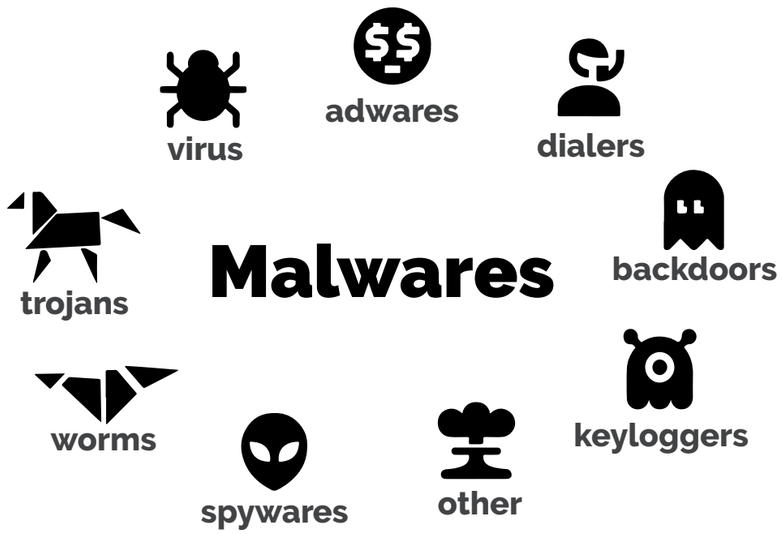
Figura 2. Tripé da cibersegurança[2]

2. Fonte: https://colaborae.com.br/blog/2022/07/29/planejamento-risco-e-incerteza/

Dica: O Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards and Technology* – NIST) dos Estados Unidos fornece o documento NIST 7298 com a definição de termos da área de segurança e informação. O/A professor/a poderá reunir os termos mais significativos e repassar aos/às alunos/as para que estejam sempre ao alcance durante o curso, em caso de dúvidas.

https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf

Figura 3. Tipos de malwares[3]



Futuro: A digitalização de vários setores da sociedade faz com que novos desafios surjam do ponto de vista da cibersegurança. Veja nesse post, os quatro principais desafios que serão enfrentados no futuro da área.

https://www.activesolutions.com.br/blog/desafios-para-o-futuro-da-ciberseguranca/

Dica: Veja os tipos de malwares mais comuns e utilizados atualmente e como podemos reconhecê-los. O/A professor/a poderá propor pesquisas em grupo no sentido de caracterizar tipos específicos de malwares. Por exemplo: quando foram criados, com qual propósito, como atuam, como podem ser evitados etc.

https://www.upguard.com/blog/types-of-malware

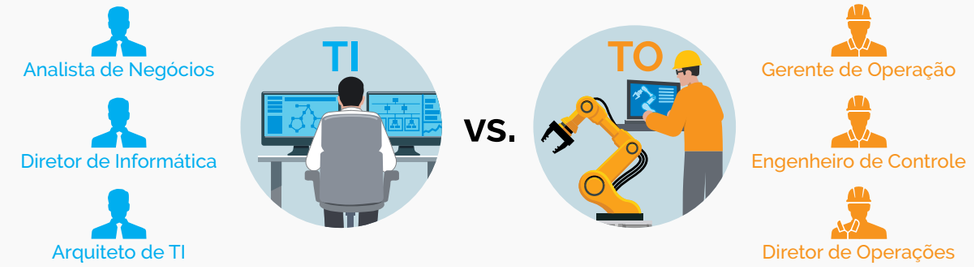
3. Fonte: https://lisata.com.br/blog/malware-voce-sabe-o-que-e/

Por se tratar de um e-book com foco no setor elétrico, é importante que os/as discentes entendam a diferença entre Tecnologia da Informação (TI) e Tecnologia da Operação (TO). De maneira simplificada podemos considerar que a TI é a infraestrutura responsável pelo controle e gerenciamento do fluxo de informações, enquanto a TO é responsável pelas operações de processos físicos e dos equipamentos utilizados para realizá-las.

Como exemplo, podemos fazer um paralelo com uma empresa do setor elétrico, mais especificamente uma empresa de geração de energia. A equipe de TI é responsável pelo fluxo de informações do ambiente corporativo: dados confidenciais, infraestrutura para trabalho remoto, assinaturas digitais, banco de dados, entre outros. Enquanto a equipe de TO é responsável por assegurar o funcionamento da geração de energia em si: usinas, máquinas, sensores, motores, painéis de monitoramento, manutenção remota etc.

Em termos de cibersegurança, a Figura 4 apresenta as diferenças entre TI e TO de maneira simplificada, mas abrangente, facilitando o entendimento sobre as medidas de cibersegurança para o setor elétrico, que serão apresentadas nos capítulos seguintes.

Figura 4. Diferença da cibersegurança entre TI e TO. [4]

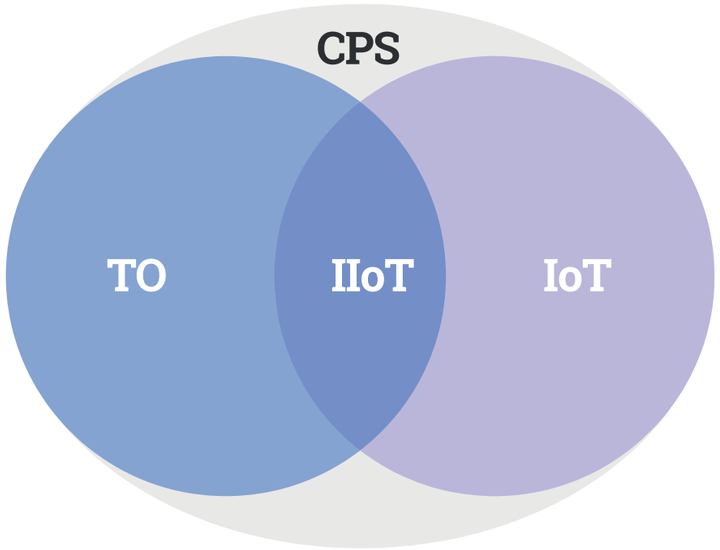


Prioridade nº 1	Confidencialidade	Disponibilidade
Foco	Integridade dos dados é a chave	Processos de controle não poem tolerar inatividade
Alvo de Proteção	Computadores pessoais e servidores	Dispositivos industriais legados, leitores de código de barras
Condições Ambientais	Ar-condicionado	Temperaturas, vibrações e impactos extremos

No passado TI e TO eram áreas diferentes com limites bem estabelecidos. Porém, o crescimento de dispositivos conectados que resultou em IoT (*Internet of Things*) industrial (IIoT – *Industrial Internet of Things*), acelerou a convergência dos outrora separados domínios de TI e TO. Consequentemente, muitas das técnicas para mitigação de riscos de segurança que serão apresentadas neste e-book, voltados para TO, são metodologias adaptadas da área de TI. Ainda, outro termo que surge com o advento da tecnologia e conectividade no setor industrial é o Sistema Cibernético-Físico (em inglês, *Cyber-Physical System* – CPS) que abrange todos os sistemas que interagem de alguma forma com o mundo físico através de ambientes cibernéticos. Exemplos disso são os sistemas autônomos automobilísticos, piloto automático na aviação e *smart grids*. A Figura 5 apresenta um diagrama da relação entre TO, IoT, IIoT e CPS.

4. Fonte: https://www.asmag.com/showpost/28556.aspx

Figura 5. Relação entre TO, IoT, IIoT e CPS[5].



A Tabela 1 traz uma comparação entre TI e TO.

Tabela 1. Comparação entre TI e TO e os impactos das diferenças para o TO[6].

Comparação	TI	TO	Impacto para TO
Ambiente de Operação	Escritório ou sala de servidor. Ar-condicionado e protegido contra poeira. Fornecimento de energia contínuo e disponibilidade de internet.	Fábricas, usinas, ambientes hostis. Poeira, temperaturas extremas, vibrações, ruídos. Fornecimento de energia e acesso à internet podem ser limitados, o que demanda a utilização de equipamentos mais eficientes e específicos	A infraestrutura de TO deve adequar-se em termos de tamanho de dados para comunicação remota devido à limitação de acesso à internet. Além disso, estratégias de mitigação para sistemas de TI podem não ser implementáveis devido aos altos requerimentos de performance.
Tecnologia	Dispositivos e programas com protocolos de comunicação padronizados e produtos comerciais "de prateleira".	Programas, dispositivos, protocolos de comunicação proprietários, o que limita a integração destes dispositivos e o suporte pode ser escasso.	A empresa fica dependente dos fornecedores para reposição de componentes, suporte ao *software* e *firmware*, antivírus, entre outros.
Ciclo de vida e dinamismo	Manutenção semanal. Ciclo de vida de 3-5 anos com suporte do fornecedor. Infraestrutura escalável e flexível com centenas ou milhares de componentes.	Ciclo de vida de décadas, com tempo de suporte inferior a isso. Manutenções esporádicas com maior mobilização devido à necessidade de interromper os processos. Topologia estática com pequena quantidade de componentes.	*Software* e *firmware* desatualizados devido ao tempo de operação ser maior que o tempo de suporte. Vulnerabilidade nos tempos atuais com a convergência da TI para a TO.
Mentalidade de projeto	Departamentos de TI dedicados. Projetado para a tecnologia baseada na internet.	Projetado do ponto de vista do *hardware*. Conexão com a internet não considerada antigamente no projeto de uma infraestrutura de TO.	Com a integração de infraestrutura de TO à sistemas de TI e conexão à internet, as vulnerabilidades de TI passaram a ser pontos críticos em sistemas de TO.
Prioridade nas operações	Eficiência e usabilidade dos sistemas. Confidencialidade, disponibilidade e integridade de dados.	Disponibilidade, resiliência e determinismo dos sistemas. Integridade dos dados e transmissão em tempo real dos dados sem atraso no envio e recebimento de dados.	Resiliência dos sistemas e proteção aos dados exigem prioridades e controles diferentes, que precisam ser incorporados quando da integração da TI à TO.

5. Fonte: https://www.missionsecure.com/ot-cybersecurity
6. Fonte: Adaptado de https://fluchsfriction.medium.com/why-ot-has-different-needs-than-it-18ba9baa36e7

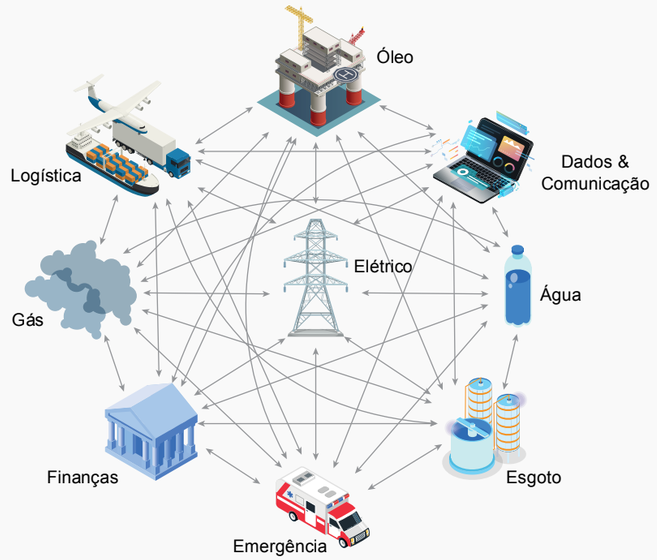
1.2. Visão sistêmica do setor elétrico, identificação de fonte de dados e potenciais riscos de segurança

A cibersegurança torna-se extremamente relevante quando consideramos infraestruturas críticas.

Saiba Mais: Definição de infraestrutura crítica no Brasil: "São as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional" (*Incisos de I a V do art. 3º da Portaria Nº 02 do GSI-PR, de 8 de fevereiro de 2008).

O setor elétrico é considerado uma infraestrutura crítica devido à "capilaridade" dos seus serviços na sociedade e a dependência deste para o desenvolvimento de outras áreas.

Figura 6. Interdependência do setor elétrico na sociedade[7]



7. I. P. d. Siqueira, REDES DE INFRAESTRUTURAS CRÍTICAS - Análise de Desempenho e Riscos dos Setores de Energia, Petróleo, Gás, Água, Finanças, Logistica e Comunicações., Rio de Janeiro: Interciencia, 2013.

Considerando a criticidade do setor elétrico, é importante entender a evolução tecnológica desse setor para compreender os desafios em implementar estratégias de cibersegurança em empresas desse ramo.

Dica: O/A professor/a pode propor seminários com o objetivo de apresentar em detalhes a evolução tecnológica do setor elétrico. Dividir a turma em grupos, para que cada grupo seja responsável por apresentar o estado da tecnologia do setor elétrico em cada período determinado.

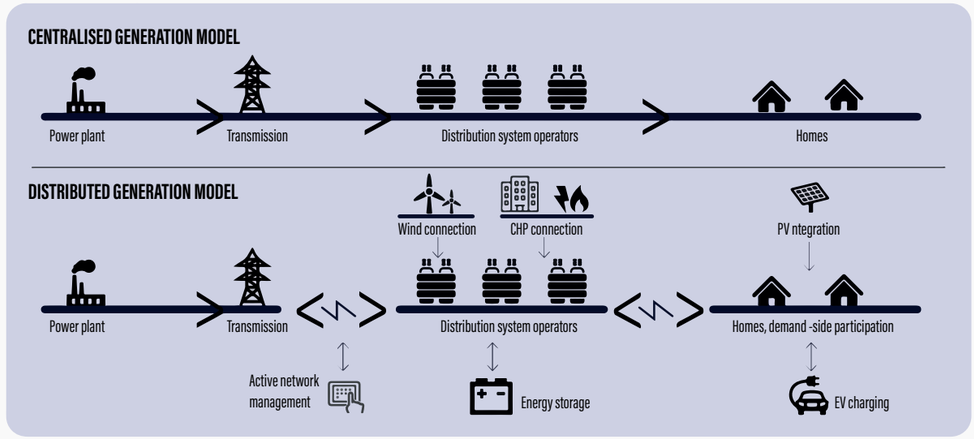
Até os anos 2000, o sistema de geração era predominantemente centralizado e com fluxo de energia unidirecional da usina para os consumidores. A energia era gerada por grandes usinas localizadas distantes dos consumidores finais e estes consumidores atuavam passivamente, ou seja, apenas consumiam a energia disponibilizada na rede elétrica. Além disso, os centros de geração, transmissão e distribuição estavam expostos apenas ao operador da rede, com protocolos de comunicação proprietários entre os equipamentos e sem muita tecnologia de integração. Assim, as vulnerabilidades eram mais físicas do que cibernéticas.

Entre os anos 2000 e 2010, houve um período de transição na automatização dos sistemas elétricos, além da migração de um sistema centralizado para distribuído e com fluxo de energia bidirecional. Em 2003, a publicação da norma IEC-61850 [4] (que estabelece protocolos de comunicação para equipamentos de subestações elétricas, o que permitiu uma maior integração entre equipamentos de diferentes empresas e a evolução da tecnologia de energias renováveis, principalmente de sistemas fotovoltaicos e eólicos) e a Resolução Normativa nº 482/2012 da ANEEL possibilitaram a geração de energia pelo consumidor, descentralizando a geração de energia e permitindo ao consumidor injetar energia na rede elétrica.

Após 2010, com a consolidação de padrões de protocolos de comunicação e desenvolvimento de novas tecnologias como medidores inteligentes, veículos elétricos, *big data* e computação baseada em nuvem, a integração tornou-se a peça-chave para um gerenciamento da rede elétrica otimizado. A Figura 7 ilustra a transição do sistema elétrico de um formato centralizado para distribuído.

É fundamental que fique claro para os/as alunos/as a correlação entre a evolução da tecnologia, a aplicação destas evoluções no setor elétrico e o impacto disso na cibersegurança das organizações. Ao decorrer da disciplina, muitas das técnicas e metodologias para prevenção de ciberataques e aumento da cibersegurança que serão apresentadas, são justificadas ou originam-se a partir do contexto apresentado nesta seção.

Figura 7. Transição do sistema elétrico de centralizado para distribuído[8]



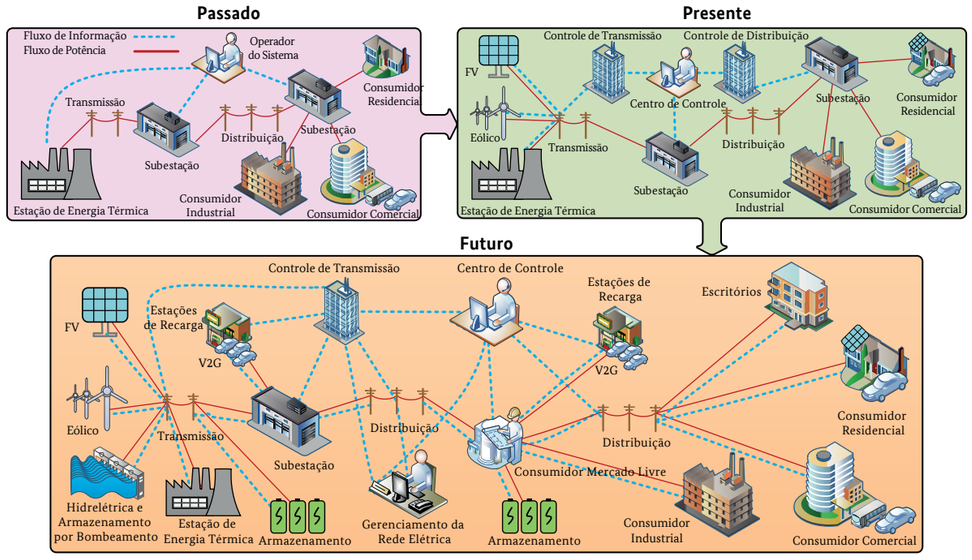
Saiba Mais: Definitivamente a penetração de sistemas de geração distribuída no sistema elétrico traz consigo inúmeras vantagens para o consumidor, para o operador da rede elétrica e para o meio ambiente. Entretanto, oferece alguns riscos relacionados à cibersegurança. Saiba mais sobre isso neste vídeo do Laboratório Nacional de Energia Renovável (*National Renewable Energy Laboratory* – NREL):

https://youtu.be/hqm1MhJJ1_k

O termo Internet das Coisas (IoT, do inglês *Internet of Things*) diz respeito a todo o dispositivo que está conectado a uma rede de comunicação de forma que as informações que trafegam por essa rede, originadas pelos dispositivos a ela conectada, possam ser acessadas por qualquer elemento da rede de maneira simples e rápida. Os equipamentos e dispositivos utilizados em infraestruturas do setor elétrico e que possuem tal funcionalidade se enquadram no termo Internet da Energia (IoE, do inglês *Internet of Energy*) [5].

8. Elaine Knutt, "Why the DSO transition must accelerate," Utility Week. Disponível: https://utilityweek.co.uk/dso-transition-must-accelerate/. [Acesso em 06 11 2021].

Figura 8. Transição do sistema elétrico com a IoE e perspectivas futuras de integração dos atores participantes [9]



Futuro: A IoE pode oferecer novos serviços e aplicações no sistema elétrico, entretanto também há os desafios tecnológicos e de segurança. Uma nova abordagem, dada a quantidade de dados disponibilizados pelos equipamentos que compõem o sistema elétrico, é a computação baseada em nuvem (*Cloud Computing*), a qual permite tomadas de decisão, gerenciamento dos ativos e gerenciamento ótimo de energia. Veja mais em:

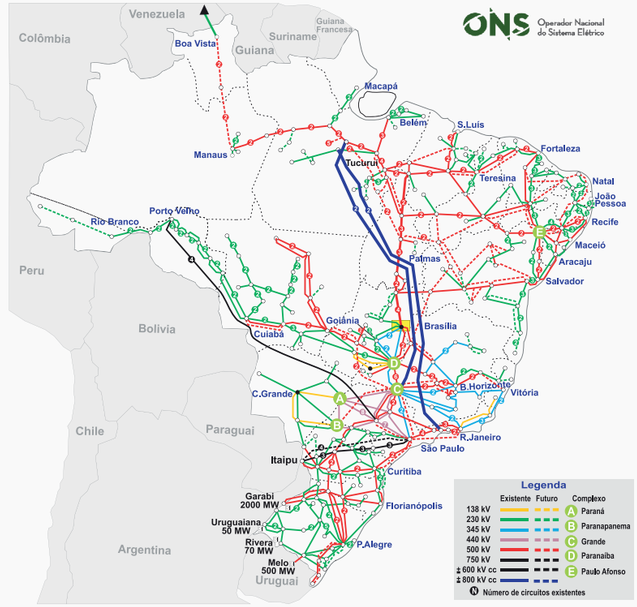
https://ieeexplore.ieee.org/document/6809180

No Brasil, o Operador Nacional do Sistema Elétrico (ONS) coordena e controla as operações de geração e transmissão do Sistema Interligado Nacional (SIN) através do relacionamento com diversos agentes do setor, como empresas públicas e privadas de geração, transmissão e distribuição de energia elétrica.

Apesar de o ONS demonstrar avanço tecnológico em termos gerenciais, com o Sistema Aberto de Gerenciamento de Energia (SAGE), ao mesmo tempo oferece vulnerabilidade em uma infraestrutura considerada crítica, uma vez que o ONS interage compartilhando informações com todos as empresas de geração e transmissão de energia elétrica conectadas ao SIN. Dessa forma, a infraestrutura de TI do ONS pode ser uma porta de entrada para demais empresas.

9. H. Shahinzadeh, J. Moradi, G. B. Gharehpetian, H. Nafisi and M. Abedi, "Internet of Energy (IoE) in Smart Power Systems," 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI), pp. 627-636, 2019.

Figura 9. Mapa do sistema de transmissão brasileiro[10]



Dica: O Grupo de Estudos do Setor Elétrico (GESEL) da Universidade Federal do Rio de Janeiro publicou um texto de discussão sobre a segurança cibernética do setor elétrico brasileiro, destacando os desafios regulatórios e tecnológicos. É sugerido ao/à professor/a que repasse aos/às alunos/as este material para complementar a visão sistêmica do setor elétrico em relação à cibersegurança. O GESEL é um grupo de estudos de referência no Brasil e este material oferece uma análise detalhada do estado atual do setor, das regulamentações e o que é sugerido para o futuro.

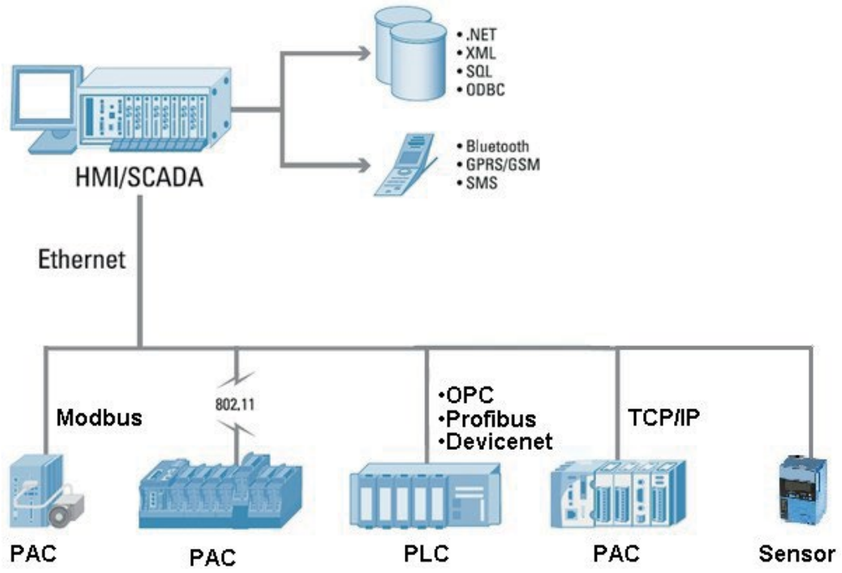
http://www.gesel.ie.ufrj.br/app/webroot/files/publications/59_TDSE_103.pdf

1.3. Padrões de protocolos de comunicação

O estabelecimento de padrões de protocolos de comunicação favoreceu a integração de equipamentos de diferentes fabricantes em uma infraestrutura de modo que o gerenciamento e controle do local pudesse ser realizado através de um único *software*. Estes dispositivos capazes de se comunicarem em uma mesma rede física aumentando a automatização do sistema são denominados Dispositivos Eletrônicos Inteligentes (IEDs, do inglês *Intelligent Electronic Devices*). Já o *software* mencionado que tem a capacidade de receber as informações destes IEDs através de uma rede de comunicação, gerenciá-los e controlá-los é denominado sistema SCADA (Sistema de Supervisão e Aquisição de Dados, do inglês *Supervisory Control And Data Acquisition*).

10. Fonte: http://www.ons.org.br/Mapas/Mapa%20Sistema%20de%20Transmissao%20-%20Horizonte%202024.pdf - Operador Nacional do Sistema - ONS [Acesso em 11 2021].

Figura 10. Exemplo de infraestrutura utilizando um sistema SCADA com IEDs[11]



Dica: Um sistema com arquitetura SCADA pode reunir IEDs com diversos protocolos de comunicação em um mesmo barramento de comunicação como TCP/IP, Modbus, Wi-Fi (IEEE 802.11), Profibus etc. Como sugestão de atividade, o/a professor/a pode propor a apresentação de protocolos de comunicação para debates sobre aspectos de cibersegurança relacionados à aplicação apresentada (vulnerabilidades, riscos, ameaças etc.).

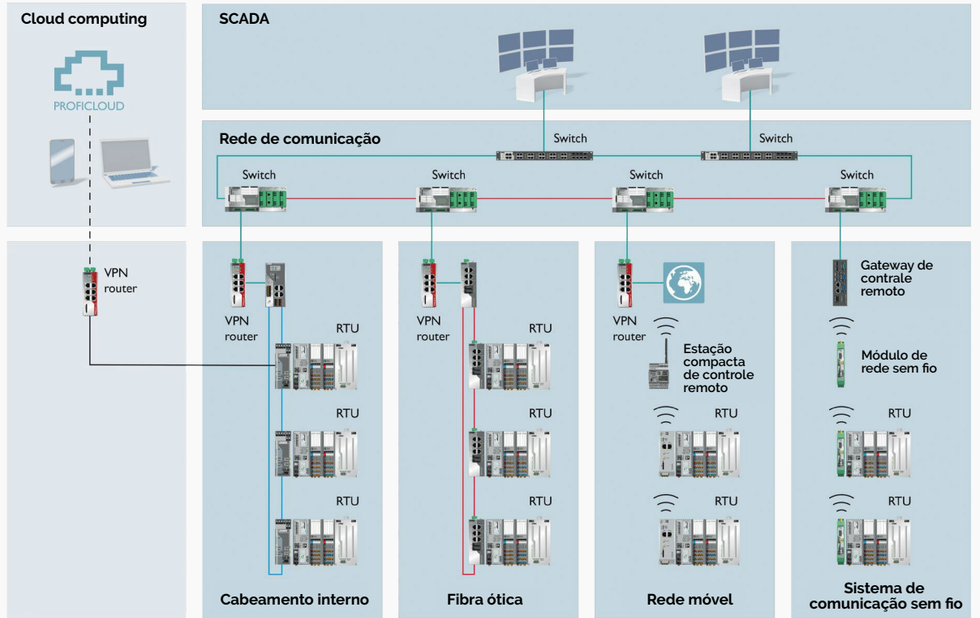
Futuro: Com a integração de IEDs e exposição destes sistemas à internet, as infraestruturas estão cada vez mais sendo aprimoradas com relação à cibersegurança. A interligação entre o sistema SCADA e os IEDs será realizada através de equipamentos como Firewalls, Routers VPN (*Virtual Private Network*), Routers de Segurança, Switches Gerenciáveis. Estes equipamentos desempenham a função de prover camadas de segurança físicas ao sistema, controlando o tráfego de dados na rede de comunicação e verificando as autorizações de acesso de cada usuário.

https://blog.netwrix.com/2019/01/22/network-security-devices-you-need-to-know-about/

https://www.cisco.com/c/en/us/products/security/what-is-network-security.html#~how-network-security-works

11. PROFIBUS Brasil, "5 Perguntas para fazer ao seu fornecedor de ferramentas SCADA,". Disponível: https://www.profibus.org.br/news/fevereiro2012/tutorial. [Acesso em 07 11 2021].

Figura 11. Exemplo de infraestrutura de comunicação industrial segmentada com dispositivos de segurança e diferentes meios de comunicação[12]



Dica: Veja mais sobre os principais protocolos de comunicação utilizados na indústria. No livro citado a seguir, os protocolos de comunicação são divididos conforme seus principais propósitos, por exemplo, protocolos para aplicações automotivas, sistemas de potência etc. É um ótimo material para disponibilizar aos/às alunos/as que não tenham muita experiência em protocolos de comunicação industriais ou que desejam aprender mais sobre o assunto.

Zurawski, Richard. Industrial Communication Technology Handbook. CRC Press, 2017. Segunda edição. ISBN 9781351831376.

Como dito anteriormente, o ONS é o responsável pelo gerenciamento e controle da geração e transmissão de energia do Brasil através do SIN. Para tal, o Operador também faz uso de um sistema SCADA para agregar os dados de interesse em uma tela/interface e possibilitar as tomadas de decisões. O sistema SCADA/EMS (*Supervisory Control and Data Acquisition/Energy Management System*) que o ONS utiliza é denominado SAGE (Sistema Aberto de Gerenciamento de Energia) e este sistema também é disponibilizado para as empresas de geração e transmissão que tem relacionamento ou operam em conjunto com o ONS [6].

12. Phoenix Contact, "Meios de transmissão e protocolos de comunicação,". Disponível: https://www.phoenixcontact.com/online/portal/br?uri=wcm%3Apath%3A/brpt/web/main/solutions/subcategory_pages/Remote_control_remote_maintenance_transmission_media_protocols/78276a78-9c9e-47cc-ae85-b2a18f8e1e2c. [Acesso em 07 11 2021].

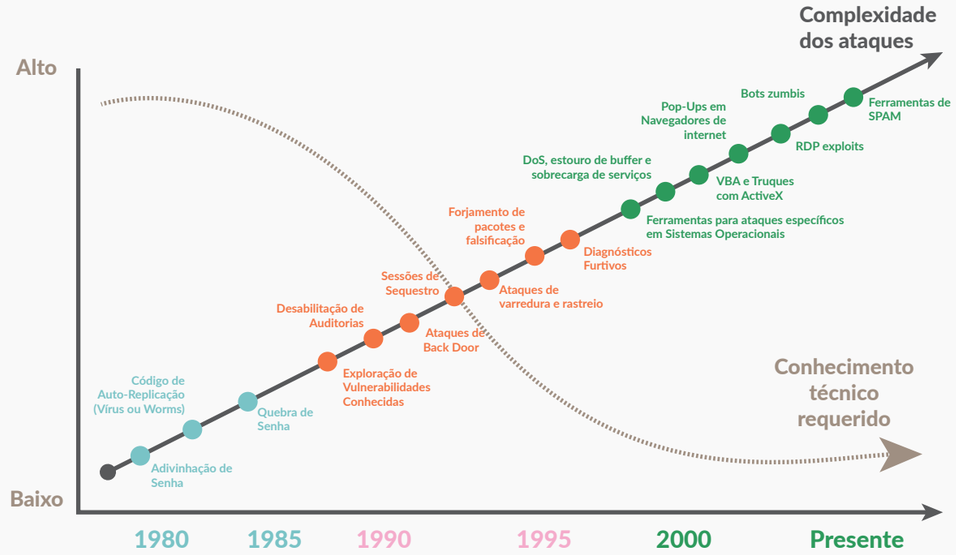
Figura 12. Sistema SAGE utilizado pelo ONS[13]

1.4. Proteção contra *malwares*

Apesar do desenvolvimento de novas tecnologias e estratégias para proteção de infraestruturas contra ciberataques, as ferramentas disponibilizadas na internet para realização de tais ataques requerem cada vez menos conhecimento técnico do criminoso. Essas ferramentas, denominadas *toolkits*, permitem que um usuário sem conhecimento técnico avançado consiga realizar ataques cibernéticos cada vez mais sofisticados.

13. ONS, "Operador Nacional do Sistema Elétrico," [Online]. Disponível: http://www.ons.org.br/. [Acesso em 07 11 2021].

Figura 13. Conhecimento técnico requerido para execução de ciberataques versus complexidade dos ataques[14]



Atualmente há diversos programas disponíveis no mercado que auxiliam o usuário a se prevenir contra possíveis ataques de *malwares*. Estes programas podem funcionar por análise ou comparação. Os que operam por análise examinam continuamente a atividade gerada por aplicativos em um dispositivo, determinando se este é um *malware* ou não. Já os programas anti-*malwares* que operam por comparação, verificam se determinados arquivos possuem assinaturas similares a *malwares* já conhecidos.

Saiba Mais: Apenas programas anti-malwares não são suficientes para a proteção do usuário ou empresa. Como os malwares estão sendo modificados e aprimorados constantemente, estes programas podem não detectar imediatamente um novo malware. Além disso, considerando um ambiente colaborativo, como uma empresa, em um caso de detecção tardia de um ataque por malware, outros dispositivos desta rede podem ter sido infectados. Portanto, não há uma única contramedida na proteção contra malwares.

Um conjunto de medidas deve ser implementado nas empresas para que a proteção contra ciberataques seja mais robusta e resiliente, uma vez que as ameaças e vulnerabilidades podem surgir de várias maneiras como falhas de *software*, falhas humanas ou falhas de *hardware*. Dessa forma há seis passos genéricos que podem ser seguidos para uma proteção efetiva contra *malwares* [7]:

14. J. J. Gonzalez, "Towards a Cyber Security Reporting System – A Quality Improvement Process," International Conference on Computer Safety, Reliability, and Security, pp. 368-380, 2005.

- Criar um programa educacional para os colaboradores serem conscientizados sobre a segurança da informação;
- Promover a divulgação de informações relacionadas à novos *malwares* (como atuam, como evitar e quais as consequências);
- Orientar os usuários sobre a transferência de arquivos de fonte desconhecida, estabelecendo regras claras de segurança caso seja necessário efetuar tal procedimento;
- Caso seja necessário testar novos programas ou abrir arquivos desconhecidos, utilizar computadores em quarentena, isolados da infraestrutura da empresa;
- Instalar anti-*malwares*, mantendo sua versão atualizada e realizando escaneamentos no sistema de forma periódica;
- Orientar (ou forçar) os colaboradores a utilizarem credenciais (*login* e senhas) fortes para processos de autenticação.

Saiba Mais: Como dito, os malwares estão em constante desenvolvimento e atualmente há aqueles que se utilizam de algoritmos de Inteligência Artificial (IA) para realizar seu propósito, de forma que, dependendo do ambiente em que se encontram, podem alterar sua estrutura para se espalhar de formas diferentes e passarem desapercebidos por programas de detecção de malwares.

https://www.uol.com.br/tilt/noticias/redacao/2021/12/21/apelidado-de-tardigrado-malware-indestrutivel-ameaca-a-biotecnologia.htm

Saiba Mais: Assim como os malwares que se utilizam de IA, há também o desenvolvimento de programas anti-malwares que utilizam a IA para melhorar a eficiência na detecção e remoção de malwares em sistemas operacionais.

https://www.securityreport.com.br/overview/deepray-inteligencia-artificial-para-combater-o-cibercrime/

https://www.acronis.com/en-eu/articles/advanced-malware-protection/

A grande maioria dos *malwares* existentes foram projetados para atuarem em redes de TI. Entretanto, a integração de infraestruturas de TO à internet fez com surgissem *malwares* específicos para este tipo de rede. Os meios para infectar uma rede de TO com *malware* é basicamente a mesma utilizada para infraestruturas de TI, atacando vulnerabilidades em redes fracas ou usuários imprudentes.

A maneira como o *malware* para TO opera depende muito das características do sistema de controle tido como alvo. Em caso de sistemas operados remotamente via *softwares* de supervisão, o invasor pode querer ganhar algum nível de controle no gerenciamento do sistema para esconder alarmes, modificar configurações, entre outros. Além disso, estes *malwares* podem atacar um dispositivo em particular, por exemplo, CLPs (Controladores Lógicos Programáveis) para alterar sua lógica de operação e, dessa forma, prejudicar os processos da empresa.

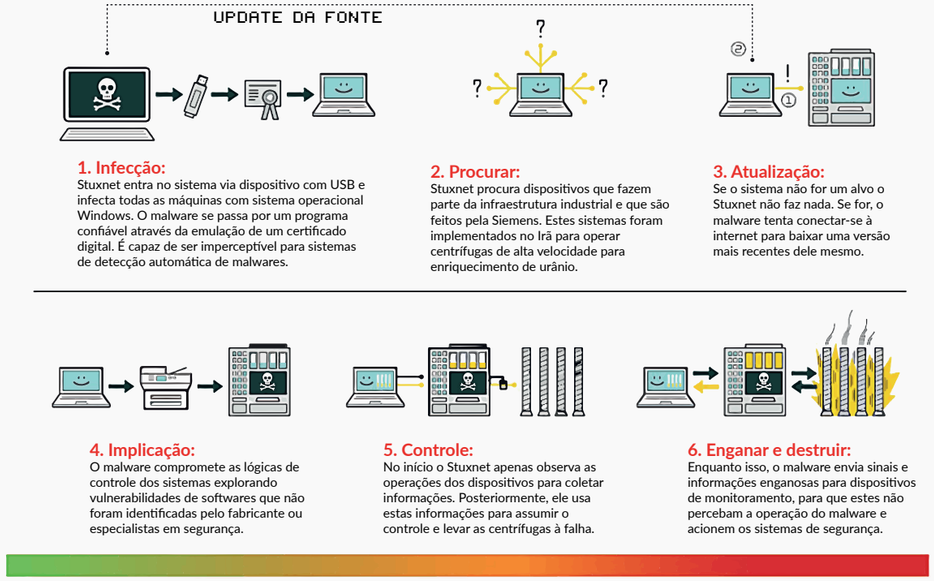
Alguns exemplos de *malwares* para TO:

- **Stuxnet:** projetado para danificar o processo de enriquecimento de urânio do Irã através de modificações em CLPs da Siemens. A Figura 14 apresenta como este *malware* opera.
  Link: https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

- **CrashOverride:** envolvido em ataques ao sistema elétrico de transmissão da Ucrânia. Este *malware* utilizou de protocolos de comunicação padronizados, como a IEC 61850, para interagir com a rede. Alterou a configuração de relés de proteção de forma que estes não operassem corretamente.
  Link: https://www.cisa.gov/uscert/ics/alerts/ICS-ALERT-17-206-01

- **Havex e BlackEnergy2:** Havex tem como função procurar e listar os tipos de servidores de TO e suas configurações. Já o BlackEnergy2 explora vulnerabilidades de IHM (Interface Homem Máquina) de forma a endereçá-las à internet e ficarem exposta.
  Link 1: https://www.cisa.gov/uscert/ics/advisories/ICSA-14-178-01
  Link 2: https://www.cisa.gov/uscert/ics/alerts/ICS-ALERT-14-281-01B

Figura 14. O modo de operação do malware Stuxnet. [15]



15. Fonte: https://medium.com/@larong2122/stuxnet-the-game-changing-malware-3535ff76a2ac

1.5. Recapitulando

Ao final deste capítulo, o/a aluno/a deverá ser capaz de:

- Entender com clareza os conceitos e termos de cibersegurança, sendo capaz de diferenciar ameaças de vulnerabilidades;
- Entender as potenciais vulnerabilidades de segurança do sistema elétrico, considerando seu estado atual de avanço tecnológico;
- Saber diferenciar os protocolos de comunicação utilizados no setor elétrico e entender como funcionam as infraestruturas de controle e monitoramento baseadas em sistemas SCADA;
- Conhecer as ferramentas disponíveis e estratégias utilizadas para proteção contra *malwares*.

Atividades Sugeridas:

- Apresentações expositivas em slides dos conceitos e definições, por exemplo: dos tipos de *malwares* (alvos, prejuízos causados, principais meios de proteção), protocolos de comunicação no setor elétrico, sistemas SCADA e programas anti-*malwares*;
- Apresentação de vídeos para consolidação dos conceitos e novidades relacionadas aos temas desta aula. Exemplos:
  - https://youtu.be/n8mbzU0X2nQ
  - https://youtu.be/hqm1MhJJ1_k
  - https://youtu.be/j0ZQc3tJCwQ
- Promover atividades em grupo e individuais, tais como seminários, para avaliação do aprendizado: seminários sobre *malwares* e seus prejuízos no setor elétrico, o impacto das tecnologias do setor de energia (Ex.: *smart meters*, geração distribuída, automação residencial, etc.) em termos de cibersegurança.

Algumas fontes interessantes:

- https://www.canalenergia.com.br/tag/ciberseguranca
- https://cybersecurityguide.org/industries/energy/
- https://cybersecurity.ieee.org/
- **Zurawski, Richard. *Industrial Communication Technology Handbook*. CRC Press, 2017. Segunda edição. ISBN 9781351831376.**
- **Brooks, C. j. *Cybersecurity Essentials*. 2018**
- **Kim, D. *Fundamentos de Segurança de Sistemas de Informação*. 2014**
- **Brown, L. *Segurança de computadores*. 2013**

Avaliação

A evolução tecnológica e a digitalização do setor elétrico, possibilitou aos consumidores de energia elétrica tornarem-se “prosumidores”, ou seja, não são mais atores passivos que apenas consomem energia, há também aqueles que geram energia e injetam a quantidade que não utilizam na rede elétrica. Isso é possível devido principalmente aos sistemas fotovoltaicos que estão mais acessíveis financeiramente hoje em dia, e são regulamentados pela ANEEL.

Diante deste contexto e da visão do setor elétrico acerca da cibersegurança apresentada neste capítulo, discorra sobre as vulnerabilidades e fontes de risco para a segurança do sistema elétrico diante da transformação da rede elétrica de uma topologia centralizada para uma distribuída.

Capítulo 2: Avaliação de riscos de segurança cibernética, ética e uso de dados

Nota para o/a professor/a – Anterior a implementação de estratégias para redução de riscos de cibersegurança é indispensável que o/a discente tenha ferramentas para conseguir identificar as vulnerabilidades e ameaças a serem mitigadas. Este capítulo proporcionará aos/às alunos/as a percepção dos meios disponíveis para quantificação e qualificação dos riscos. Ainda, oferece uma orientação sobre as normas internacionais e boas práticas de cibersegurança.

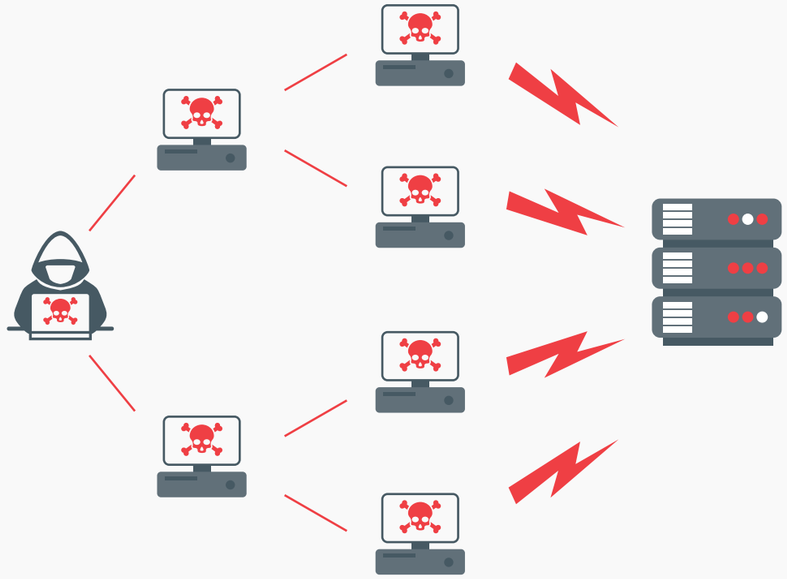
2.1. Reconhecimento e análise de vulnerabilidades e riscos

A evolução das tecnologias permite o desenvolvimento de novas aplicações e oferta de novos serviços, porém também abre espaço para novos cenários de riscos e vulnerabilidades. Para que o/a aluno/a possa aplicar medidas de proteção e contenção contra ciberataques, é necessário saber reconhecer e analisar as vulnerabilidades existentes em um sistema ou infraestrutura de comunicação.

Conforme Solomon [7], é necessário saber das motivações, propósitos, tipos de ataques e suas fases para que o/a profissional consiga avaliar o cenário da melhor forma e propor correções ou melhorias efetivas. As motivações de um ataque podem ser dinheiro, fama, crença, sistema político ou vingança. Já o propósito resume-se, basicamente a quatro pontos:

- **Negação de serviço:** negar serviços de um determinado sistema através de acessos simultâneos a este sistema (congestionamento do tráfego de informações);
- **Adulteração de dados:** modificação ou exclusão de dados ou configurações de um sistema;
- **Extração de dados:** roubo de dados ou credenciais de acesso para revenda na internet ou exposição de usuários;
- **Ponto de partida:** realização de um ciberataque em um dispositivo para usá-lo posteriormente como ponto de partida para infecção e ataque a outros dispositivos.

Figura 15. Concepção simplificada de um ataque de negação de serviço, onde vários computadores infectados realizam acesso simultâneo à um servidor ou serviço a fim de congestionar o tráfego e impedi-lo de ser acessado para seu real propósito[16].



Com relação à classificação dos ciberataques, estes são divididos em três categorias [7]:

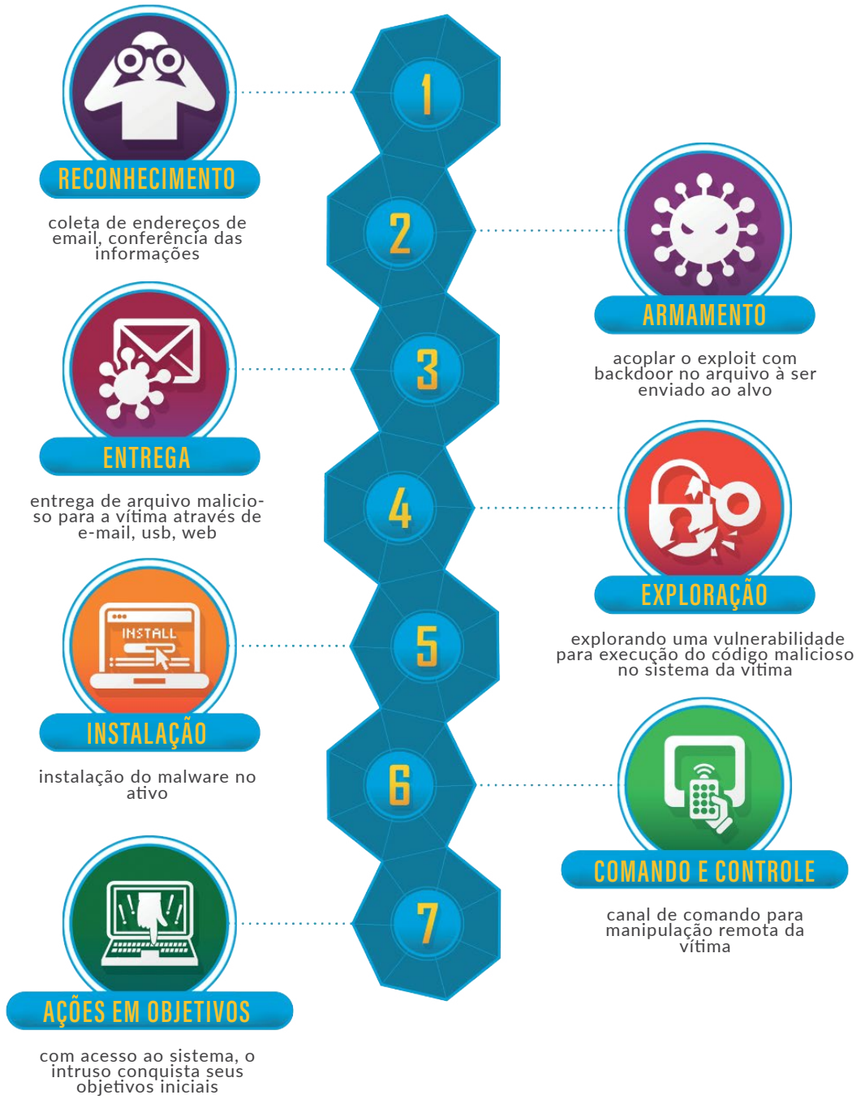
Tabela 2. Tipos de ataques cibernéticos.

Ataque	Estruturado	Desestruturado
Direto	Ataques planejados e sofisticados, realizado por um usuário (ou grupo) com habilidades técnicas avançadas, almejando um alvo em específico.	Ataques com menos sofisticação técnica, realizados por usuários menos habilidosos, almejando um alvo em específico.
Indireto	Ataques planejados e sofisticados, realizado por um usuário (ou grupo) com habilidades técnicas avançadas, sem um alvo definido. Exemplo: disponibilizar um malware na internet e esperando que algum usuário descuidado seja vítima.	Ataques com menos sofisticação técnica, realizados por usuários menos habilidosos sem um alvo definido.

Com exceção de um ataque indireto, a realização de um ciberataque pode ser dividida em fases. A divisão e denominação de cada fase está relacionada, geralmente, ao modelo adotado pelo profissional para estudo de caso. Por exemplo, há o modelo MITRE ATT&CK e o modelo da Lockheed Martin, como apresentado na Figura 16.

16. TICSS, "Firewall de Palo Alto: Esta vulnerabilidad en PAN-OS permite realizar ataques DoS,". Disponível: https://orangeitcss.net/2021/08/14/firewall-de-palo-alto-esta-vulnerabilidad-en-pan-os-permite-realizar-ataques-dos/. [Acesso em 08 11 2021].

Figura 16. Fases de um ciberataque baseado no modelo da Lockheed Martin para identificação e prevenção de ataques[17]



Saiba Mais: Conheça em detalhes a "anatomia" de um ciberataque baseado no modelo MITRE ATT&CK

https://www.countercraftsec.com/blog/post/infographic-anatomy-of-a-cyber-attack/

17. Lockheed Matin, "The Cyber Kill Chain," [Online]. Disponível: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [Acesso em 08 11 2021].

Estudo de Caso: Exemplo de um ataque de malware que comprometeu os sistemas de administração do governo dos Estados Unidos por meses. Estudos de caso como este fornecem uma visão prática de como é iniciado um ataque e quais são as complicações de situações como esta.

https://brasil.elpais.com/internacional/2020-12-29/anatomia-do-grande-ataque-cibernetico-que-comprometeu-o-eixo-da-administracao-dos-eua.html

Com o conhecimento das motivações de um ataque, propósitos, tipos e fases, é mais fácil reconhecer e analisar possíveis riscos. A análise de riscos também contempla análise de vulnerabilidade e ameaças, pois, como visto no capítulo 1, o risco é resultante das ameaças e vulnerabilidades sobre os ativos. O propósito da análise de riscos é identificar, listar e caracterizar os elementos ou fatores de risco (vulnerabilidades e ameaças) para que posteriormente seja possível fazer uma avaliação destes riscos.

O processo de análise de riscos é etapa de fundamental importância para a implementação de uma política de gestão de riscos, que será apresentada no capítulo seguinte.

A análise dos riscos presentes em uma empresa pode ser dividida em cinco etapas [8]:

- **Identificação de ativos:** processo para identificação dos ativos da organização, dispositivos e *softwares*, com informações sobre o responsável daquele ativo, modelo, fabricante e outras características;
- **Identificação de ameaças:** levantamento das ameaças por meio de registro de incidentes de segurança passados, dos responsáveis pelos ativos e usuários ou por ameaças catalogadas que façam sentido diante do tipo da infraestrutura e ativos que estão sendo analisados;
- **Identificação de controles:** processo para levantamento de controles e planos de implementação de medidas para tratamento de riscos de segurança, quando houver. Essa etapa permite uma posterior avaliação desses planos e adequação, se necessário;
- **Identificação de vulnerabilidades:** a entrada desse processo é o resultado das três etapas anteriores. O objetivo é identificar vulnerabilidades que as ameaças possam explorar diante dos ativos presentes na empresa;
- **Identificação de consequências:** por fim, esta etapa identifica as prováveis consequências de eventuais ataques com base na lista de ativos, lista de processos de negócios da empresa e lista de ameaças e vulnerabilidades correlacionadas aos ativos da organização.

Dica: O/A professor/a pode apresentar as cinco etapas de uma análise de risco de forma aplicada. Por exemplo, utilizar de sua experiência profissional para que, a cada etapa, aplique a análise juntamente com os/as alunos/as: identificação de ativos, identificação de ameaças àqueles ativos, controle e tratamento de riscos e identificação das vulnerabilidades associadas aos ativos.

A análise de riscos, também conhecida como ***threat modeling***, é um processo que deve ser realizado continuamente para detecção de novas ameaças e vulnerabilidades à medida que a infraestrutura seja modificada ou devido ao tempo de uso. Para melhor aplicar as etapas anteriormente citadas, há sete passos que podem ser seguidos.

1. **Entendimento sobre a organização e seus negócios:** é necessário que a pessoa ou equipe que fará a análise de riscos entenda a organização, conheça os negócios e processos, o mercado em que esta atua. Dessa forma, será mais fácil e assertivo identificar as possíveis ameaças e consequências de ataques;
2. **Revisão da infraestrutura física e lógica da organização:** não apenas os ativos da empresa são importantes, mas a maneira que estão sendo utilizados e interligados à infraestrutura da empresa. Esta etapa oferece a oportunidade de identificar vulnerabilidade físicas do sistema;
3. **Identificação de ativos;**
4. **Identificação de ameaças e vulnerabilidades;**
5. **Revisão das contramedidas e identificação de escopo da análise:** como dito anteriormente, quando há um plano de controle e contramedidas é necessário revisá-lo e adequá-lo sempre que necessário. Também é importante que seja identificado o escopo da análise de risco, ressaltando também o que não foi abordado. Um processo de análise de risco nem sempre conseguirá abordar tudo, seja por questões de custos ou outras limitações, por isso essa informação é relevante para futuras análises de risco;
6. **Integração do estado de segurança atual com o centro de operações de cibersegurança:** quando há existência de um centro de operações de cibersegurança, é necessário que o estado atual da cibersegurança, após uma análise de risco, seja apresentado para o centro de forma que este possa rever seus planos de atuação e contramedidas;
7. **Monitoramento contínuo e aprimoramento.**

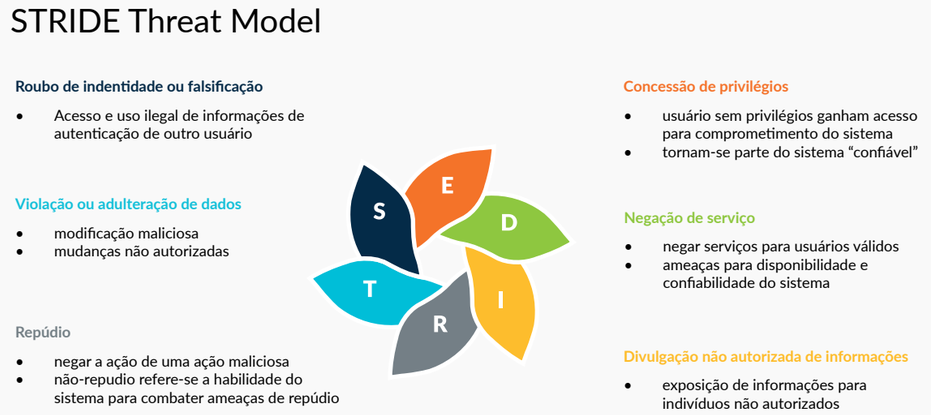
Figura 17. Etapas para uma análise de riscos de sucesso[18]

18. R. Kesavan, "THREAT MODELING RECIPE FOR A STATE-OF-THE-ART SOC," HAWKEYE, [Online]. Disponível: https://www.hawk-eye.io/2019/05/threat-modeling-recipe-for-a-state-of-the-art-soc/. [Acesso em 12 11 2021].

Saiba Mais: Há diversas ferramentas e metodologias que auxiliam na análise de riscos. Por exemplo, a Microsoft desenvolveu uma ferramenta denominada "STRIDE" a qual facilita e auxilia na identificação e classificação de ameaças.

https://semiengineering.com/five-steps-to-successful-threat-modeling/

Figura 18. Ferramenta STRIDE Model para auxílio na identificação de ameaças[19]



Saiba Mais: Apesar da grande quantidade de ciberataques e dos prejuízos que estes causam às empresas, os investimentos em cibersegurança ainda não são suficientes. As análises de risco podem ser vistas como mais um gasto no orçamento da empresa do que como investimento. Entretanto, um estudo da Cisco de 2020 [9] mostra que a cada 1 dólar investido em segurança digital, o retorno sobre este investimento é em média de US$ 2,7, chegando à US$ 3,3 quando consideramos apenas o Brasil. Além disso, uma boa análise pode servir para muito mais do que apenas cibersegurança. Veja nesse site algumas das vantagens e benefícios:

https://blogbr.clear.sale/analise-de-vulnerabilidade

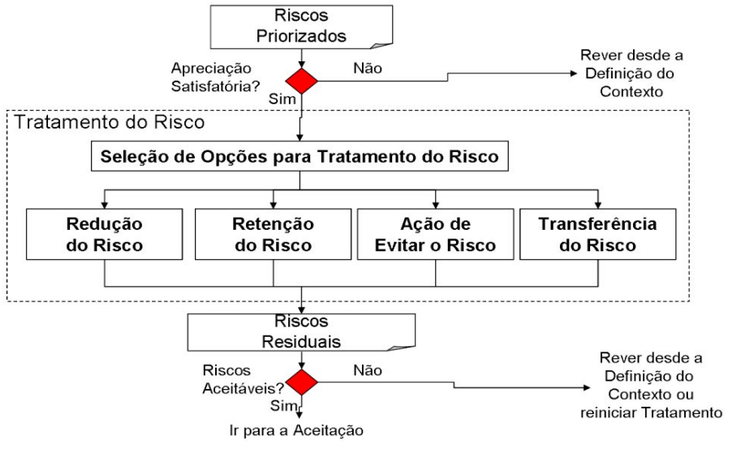
A estimativa de riscos serve para atribuir valores e consequências para cada risco levantado na análise de riscos. Segundo a ISO/IEC 27005 [10], o grau de detalhamento desta etapa depende da situação atual da organização referente à cibersegurança. Caso a empresa se encontre em um processo de primeira implantação e adequação à cibersegurança, essa estimativa de riscos deve ser feita em nível mais superficial, sem maiores detalhamentos para que não seja um processo demorado e a empresa fique exposta à ataques por mais tempo. A depender da criticidade do risco levantado e dos ativos envolvidos, é recomendado ser feito uma estimativa e análise mais detalhada.

Por fim, é realizada a avaliação dos riscos com base na análise e estimativa destes. A avaliação tem

19. SURESH MARISETTY, "Five Steps To Successful Threat Modeling," Semiconductor Engineering, [Online]. Disponível: https://semiengineering.com/five-steps-to-successful-threat-modeling/. [Acesso em 12 11 2021].

como propósito priorizar os riscos conforme sua relevância para a organização diante das consequências que podem acarretar. A Figura 19 apresenta um fluxograma para auxílio na avaliação dos riscos. É importante ressaltar que na maioria das vezes não será possível eliminar todas as vulnerabilidades e ameaças em um primeiro momento, seja por questões de custo ou por limitações de infraestrutura. Portanto, alguns destes riscos se tornam toleráveis, porém devem ser adotadas contramedidas para mitigar possíveis prejuízos.

Figura 19. Processo de avaliação e tratamento dos riscos identificados e classificados[20]



2.2. Regulamentação relacionada a uso e segurança de dados

É possível dividir em duas partes este conteúdo aos/às alunos/as: as leis relacionadas à proteção e uso de dados em geral, e as relacionadas especificamente ao setor elétrico. Não são assuntos distintos, pois as leis de uso geral complementam as que são voltadas para o setor elétrico.

Das leis de proteção e uso de dados gerais, pode ser abordada duas em específico, a Lei Geral de Proteção de Dados (LGPD) do Brasil e o Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation* – GDPR) da União Europeia. A LGPD do Brasil, Lei Nº 13.709/18, é a base jurídica para a coleta, processamento e uso de dados pessoais de pessoas físicas e jurídicas no Brasil. Essa lei foi baseada na GDPR da União Europeia que é considerada uma das mais rígidas do mundo. A Figura 20 apresenta um panorama das leis de proteção de dados no mundo com relação ao rigor de cada uma.

A LGPD, segundo o artigo 1º, "*dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural*". Ainda, empresas baseadas fora do território brasileiro, mas que atuem no país e coletam ou utilizam de alguma forma dados de cidadãos ou empresas brasileiras, devem estar em consonância com a LGPD. Figura 21 traz os principais pontos definidos na LGPD, já a forma como os dados coletados pelas empresas devem ser processados e tratados, é apresentado na Figura 22.

20. J. H. C. Fernandes, "INTRODUÇÃO À GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO," CEGSIC, Gestão da Segurança da Informação e Comunicações - GSIC, 2011.

Figura 20. Mapa mundial apresentando a rigidez das leis de proteção e uso de dados em cada pais. Para saber mais detalhes de cada pais e suas leis[21]

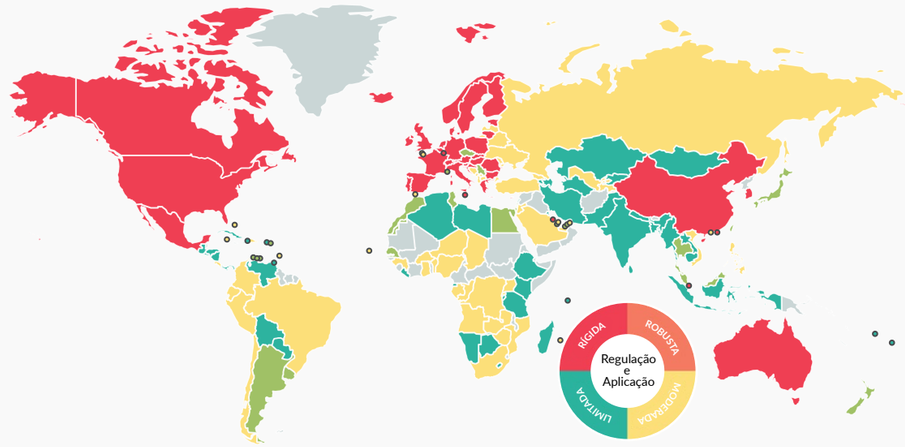
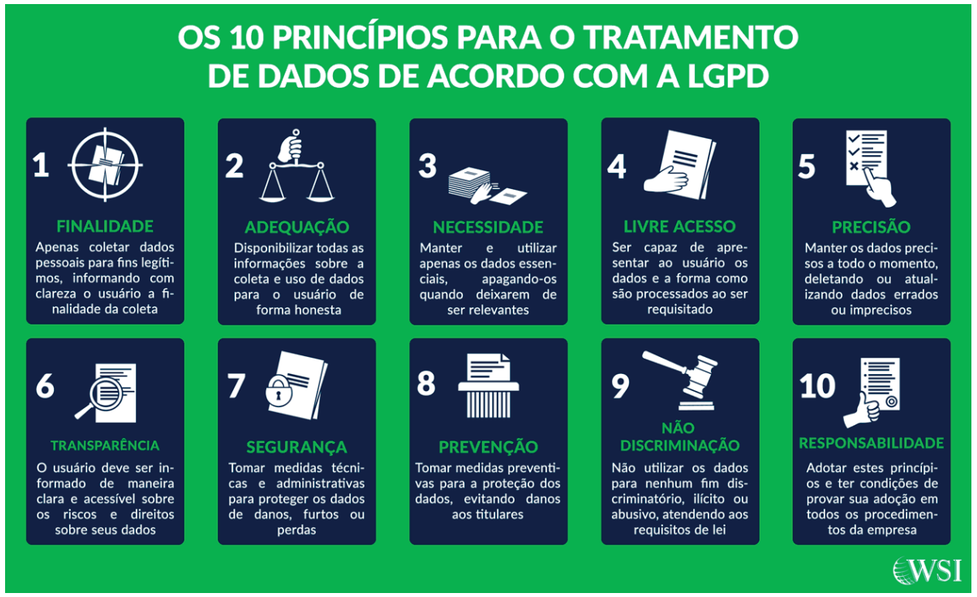


Figura 21. Pontos principais da LGPD: definições de conceitos, consentimento, transparência, fiscalização, responsabilidade e penalidades[22]

21. Acesse: https://www.dlapiperdataprotection.com/.

22. Giovana Pignati, "O que é LGPD: Lei Geral de Proteção de Dados Pessoais," Tecmundo. Disponível: https://www.tecmundo.com.br/seguranca/220645-lgpd-lei-geral-protecao-dados-pessoais.htm. [Acesso em 12 11 2021].

Figura 22. Princípios para o tratamento de dados sensíveis de acordo com a LGPD[23]



Dica: Para que os/as alunos/as tenham exemplos práticos de como a LGPD pode ser implementada, este link fornece quais são os procedimentos para que as empresas possam se adequar à LGPD e manter uma gestão de conformidade.

https://www.gat.digital/blog/gestao-de-conformidade-lgpd-guia-completo/

Ambas as regulamentações, LGPD e GPDR, estabelecem obrigações para aqueles que coletam informações de usuários. São elas:

- Possibilitar ao usuário escolher como seus dados serão utilizados se este optar por autorizar seu uso;
- Possibilitar ao usuário solicitar a exclusão de seus dados do banco de dados da organização que os possui ou a interrupção da coleta de informações;
- Apresentar de forma explícita e clara quais dados estão sendo coletados e qual a finalidade;
- Em caso de incidentes de segurança que resultem em exposição dos dados coletados, a organização responsável pela coleta e armazenamentos destas informações deve notificar as autoridades em até 72 horas; entre outros.

A Figura 23 apresenta de forma simplificada como deve ser a coleta, processamento e armazenamento de dados conforme a GDPR.

23. Caio Cunha, "LGPD: entenda o que muda com a Lei Geral de Proteção de Dados," WSI Consultoria. Disponível: https://blog.wsiconsultoria.com/lgdp-entenda-o-que-muda-com-a-lei. [Acesso em 12 11 2021].

Figura 23. A GPDR também estipula de que forma deve ser feito a coleta, processamento e armazenamento dos dados e os autores envolvidos no processo[24]

Saiba Mais: Mais detalhes sobre a GPDR podem ser obtidas através destes infográficos:

https://www.redscan.com/services/gdpr/summary/

Com relação ao setor elétrico, há diversas normas internacionais já consolidadas que estão se tornando mandatórias em alguns países. No Brasil, ainda não há uma regulamentação definida para o setor apesar de já haver grupos de estudo e comitês ligados aos órgãos governamentais responsáveis por alterações e proposições de leis e requisitos mínimos para operação segura.

A Figura 24 traz algumas das normas internacionais relacionadas à cibersegurança no setor elétrico que são utilizadas como referência no Brasil, e entidades internacionais responsáveis pela criação e normas e padrões que são considerados referência.

24. Punita & Jasmeeta, "The Cyber Break-ups - Art. 17 GDPR Right to erasure ('right to be forgotten')," Cyber Waves. Disponível: https://www.cyberwaves.eu/blog/gdpr/the-cyber-break-ups/. [Acesso em 12 11 2021].

Figura 24. Exemplos de organizações reguladoras e de normatização, e normas relacionadas à cibersegurança nos EUA e União Europeia.[25]

Saiba Mais: Apesar da inexistência de regulamentação de cibersegurança para o setor elétrico no Brasil, há normas internacionais que podem ser seguidas na implementação de infraestruturas seguras. São elas: ISA-99, IEC-62443, IEC-17799, IEC-27002, IEC-27032, IEEE-2857, IEEE-1686, IEEE-C37.240-2014, NERC-CIP-002-1 à NERC-CIP-009-1.

Saiba Mais: Diversos países têm manifestado grande preocupação com a segurança cibernética de setores críticos como o da energia. Consequentemente, várias propostas de mudança de políticas de segurança e a formação de comitês para formulação de novas regulações têm sido noticiados.

Europa: **https://www.wsj.com/articles/european-energy-sector-prepares-for-new-cybersecurity-rules-11623144602**

Estado Unidos: **https://www.energy.gov/cio/downloads/doe-cybersecurity-strategy-2018-2020**

No Brasil, o ONS submeteu à ANEEL (Agência Nacional de Energia Elétrica) em dezembro de 2019 uma proposta para operação segura do SIN, estabelecendo requisitos de cibersegurança. Após 2 anos de discussões, a ANEEL publicou em 22/12/2021 a Resolução Normativa n° 964 que trata das diretrizes de políticas de segurança cibernética para os agentes do setor.

https://www2.aneel.gov.br/cedoc/ren2021964.html

25. Adaptado de Paulo H. Soares, "Cibersegurança NOKIA," em Workshop Internacional sobre Segurança Cibernética ANEEL, Brasilia, 2016.

Saiba Mais: No Brasil, a Agência Nacional de Telecomunicações (ANATEL) publicou em janeiro de 2021 uma regulação para fabricantes e fornecedores de equipamentos para telecomunicações e IoT. Em outros países também há leis específicas para IoT. Veja mais em:

https://cetome.com/panorama

2.3. Compreensão dos aspectos éticos do uso e manipulação de dados

Cada vez mais as propagandas são direcionadas de forma personalizada aos usuários na internet. Algoritmos verificam as atividades do usuário e selecionam anúncios ou oferecem sugestões com base em seus interesses através da coleta de dados proveniente de sites, serviços que requisitam dados pessoais, *cookies*, redes sociais etc. Dessa forma, os dados pessoais acabam por se tornar uma *commodity* com alto valor para indústrias de diversos setores.

Saiba Mais: Um dos casos de violação de privacidade de usuário de maior impacto mundial foi o da empresa Facebook com a Cambridge Analytica em 2018. Os dados de milhões de usuários da rede social estavam à disposição da Cambridge Analytica, a qual utilizou-se disso para tentar influenciar o resultado das eleições para presidente dos Estados Unidos.

https://privacyinternational.org/news-analysis/2857/cambridge-analytica-gdpr-1-year-lot-words-and-some-action

Neste contexto de dependência de coleta de dados de usuários ou empresas, a observação da regulamentação vigente quanto à proteção de dados e participação humana (funcionários de uma empresa, por exemplo) no tratamento e armazenamento de dados é de suma importância, para que sejam implementadas práticas que estimulem tomadas de decisões éticas no cotidiano das empresas.

- Criar e divulgar um código de ética de forma a padronizar algumas tomadas de decisões em consonância com os valores da empresa e requisitos mínimos obrigatórios de regulamentações, conscientizar das consequências da utilização de dados e esclarecer a finalidade e objetivo do motivo que tais dados estão sendo coletados e processados;
- No momento anterior à coleta de dados, o usuário deve autorizar o ato diante de uma declaração da empresa informando a finalidade dos dados coletados. Esta etapa de consentimento do usuário deve ser mais clara e direta possível, pois é plausível que com o passar do tempo, nas etapas de tratamento e armazenamento dos dados, os termos aceitos inicialmente pelo usuário não sejam os mesmos, devido à replanejamentos estratégicos da empresa, adição de tecnologias, entre outros;
- Atualmente há diversas ferramentas automatizadas que oferecem excelentes desempenhos no processamento e utilização de dados, por exemplo, algoritmos baseados em inteligência artificial. Entretanto, deve-se ter atenção pois os resultados podem, muitas vezes, violar os termos e condições em que o usuário consentiu a utilização de seus dados.

Saiba Mais: Algumas leis de proteção de dados, como a GDPR por exemplo, apesar de estarem em vigor há algum tempo, constantemente atualizam suas definições conforme o avanço da tecnologia e das formas como o dado dos usuários são utilizados. Um aspecto de interesse é a ética relacionada ao uso de dados. O documento a seguir fornece um guia relacionado à identificação dos aspectos éticos relacionados a dados durante todo ciclo de vida de um projeto:

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf

E aqui, há um site que provê uma árvore de decisão interativa conforme o guia acima apresentado:

https://ec.europa.eu/assets/rtd/ethics-data-protection-decision-tree/index.html

Dica: A seção que tratou da evolução tecnológica no setor elétrico, permitiu ao/a aluno/a observar a possibilidade da criação e oferta de novos serviços com base na coleta de dados do usuário. Neste sentido, é interessante que o/a aluno/a tenha clareza sobre os desafios da atualidade com relação à ética de dados e a dependência cada vez maior de algoritmos para tomada de decisão com base no processamento de dados:

https://medium.com/somos-tera/o-que-e-etica-de-dados-3ce4702cdfc1

2.4. Certificação de segurança de *hardwares*

Nas seções anteriores, o/a aluno/a pôde entender sobre as regulamentações relacionadas à proteção de dados, as metodologias e práticas para a coleta, tratamento e utilização dessas informações de forma segura e preservando a privacidade do usuário. Porém, há meios físicos de contribuir para que seja adicionado camadas de segurança nesses processos e tornar todo o procedimento mais robusto frente a ataques cibernéticos ou erros humanos. Essa camada de segurança adicional é feita através de certificações de segurança de *hardwares*.

Há basicamente dois cenários em que ficam evidentes as vantagens da adição desse tipo de camada de segurança. Um cenário é a transmissão de dados do ponto de origem ao ponto de destino. Neste caminho, pode haver interceptação de dados por cibercriminosos para utilização indevida ou manipulação dos dados, por exemplo. O segundo cenário é o controle de acesso de dados sensíveis no local de armazenamento destas informações que supostamente deve ser seguro.

Para estes tipos de situações há um dispositivo físico (*hardware*) denominado Módulo de Segurança de Hardware (HSM, do inglês *Hardware Security Module*), que fornece chaves criptográficas (além de outras funções) de modo que os dados só podem ser acessados por usuários autorizados que possuam chaves criptográficas fornecidas pelo dispositivo. Há também a função de autodestruição em caso de tentativas de acesso não autorizadas. Dessa forma, é importante que a equipe de segurança faça *backups* periódicos das informações de modo a não as perder por completo em casos de ataques.

Dica: Como sugestão, o/a professor/a pode apresentar as funções dos HSMs e como cada uma contribui para a segurança dos processos, conforme as fontes auxiliares abaixo, e posteriormente propor atividades para que os/as alunos/as identifiquem aplicações para cada função para o setor elétrico.

Geração de PKI e armazenamento de chaves: **https://cryptoid.com.br/certificacao-digital/o-que-e-pki-definicao-e-guia-para-infraestrutura-de-chave-publica/**

Segurança de comunicação SSL/TLS: **https://www.hostinger.com.br/tutoriais/o-que-e-ssl-tls-https**

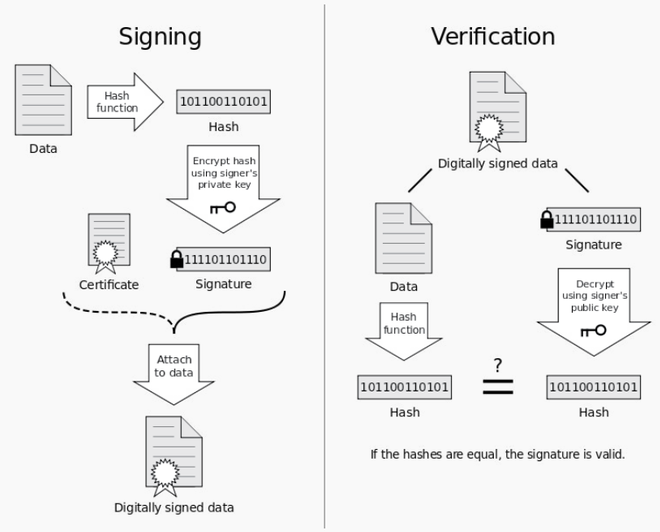
Validação de assinaturas e certificados digitais: **https://www.evaltec.com.br/assinatura-digital-assinatura-eletronica-e-certificado-digital/**

Criptografia de case de dados: **https://www.evaltec.com.br/aplicar-criptografia-com-eficacia-ainda-e-um-desafio-para-proteger-dados-de-empresas/**

Saiba mais: Devido à pandemia de Covid-19 no mundo, desde o início do ano de 2020, as empresas tiveram que adaptar seus processos considerando a presença digital de seus colaboradores. Da mesma forma, os documentos que necessitam de assinaturas por parte de seus responsáveis tiveram que se adaptar à essa nova realidade. Com isso, uma ferramenta que se popularizou foi a utilização das assinaturas digitais. Essa ferramenta utiliza HSMs para validação e comprovação das assinaturas. A Figura 25 ilustra de que forma é realizado o processo de assinatura digital.

https://blog.zapsign.com.br/verificador-de-assinatura-digital/

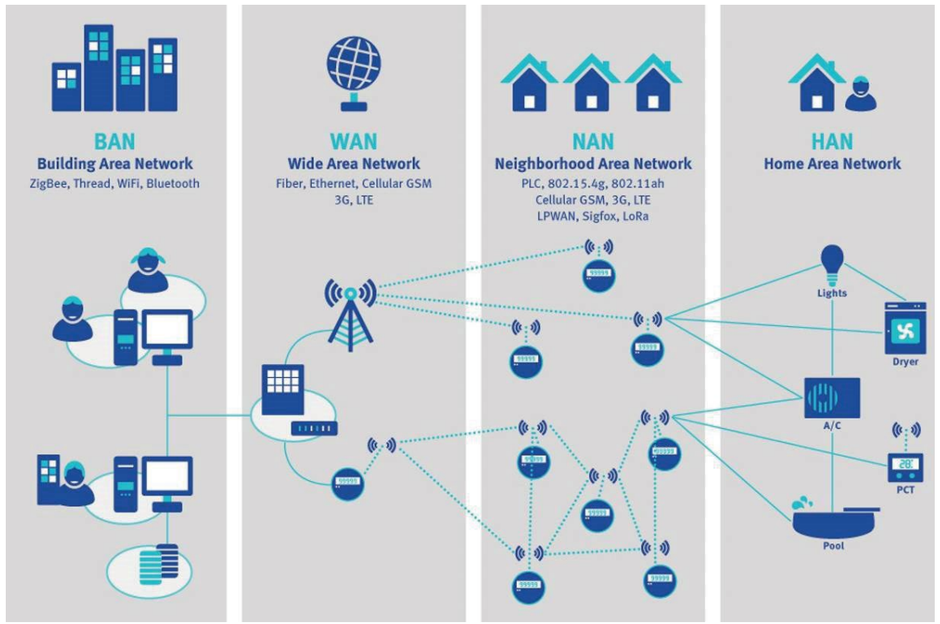
Figura 25. Processo de assinatura digital e respectiva validação. As chaves HASH são validadas através de chaves públicas que ficam sob domínio das organizações de interesse, armazenadas em HSMs. As chaves públicas são responsáveis pela validação das assinaturas digitais[26]



26. Valter de Souza, "E-mails assinados digitalmente. O que é e como funcionam as assinaturas digitais?," Mailfence. Disponível: https://blog.mailfence.com/pt/emails-assinados-digitalmente/. [Acesso em 14 11 2021].

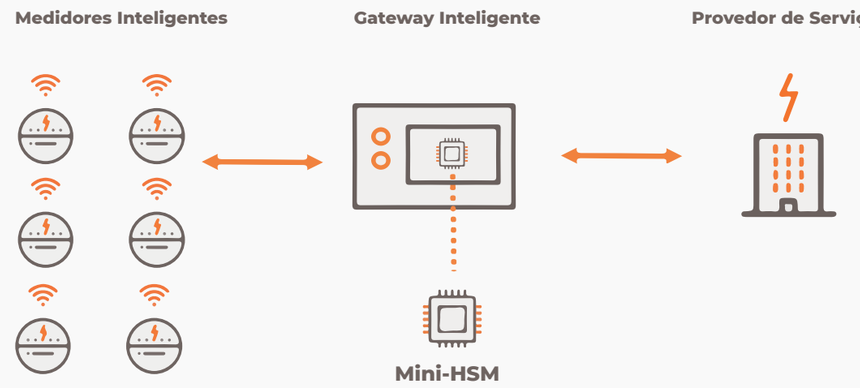
No setor elétrico, um exemplo da utilização de HSMs é o sistema de *smart metering* (medição inteligente) utilizado por empresas de distribuição de energia elétrica. Esses medidores, instalados nos consumidores, transmitem as leituras de consumo de energia via canal de comunicação sem fio, por exemplo, para a empresa responsável pela emissão da fatura de energia, como ilustra o diagrama apresentado na Figura 26. No percurso que o dado faz desde o *smart meter* até a companhia de energia elétrica, há vulnerabilidades que podem ser exploradas por criminosos a fim de manipular dados, inserir *malwares* ou furtar estes dados para venda. Dessa forma, há a possibilidade de utilizar HSM nas estações retransmissoras dos dados a fim de criptografar os dados e prover uma camada de segurança, garantindo à companhia de energia e o consumidor final que os dados sejam confiáveis e seguros. A aplicação do HSM neste contexto é apresentada na Figura 27.

Figura 26. Exemplo de infraestrutura de rede para aplicação de smart meters. Os dados aferidos pelos smart meters são enviados para estações de transmissões, ou gateways, que por sua vez enviam para a empresa de energia elétrica[27]



27. Emmanuel Gresset, "How to address the communications challenges of Smart Meters," ee News - Europe. Disponível: https://www.eenewseurope.com/news/how-address-communications-challenges-smart-meters. [Acesso em 2021 11 14].

Figura 27. Utilização de HSM na infraestrutura de transmissão de dados dos smart meters para a companhia de energia elétrica[28]



Saiba mais: Para garantir que os HSMs, independente do fabricante, sejam de fato seguros e estejam em conformidade com as normas de segurança internacionais, são emitidos certificados de segurança. Empresas especializadas e autorizadas a emitir este tipo de certificado realizam testes intensivos nos dispositivos conforme os requisitos de normas de segurança.

https://hsm.utimaco.com/blog/what-are-the-common-criteria-for-hardware-security-modules-hsms/

2.5. Avaliação dos riscos de segurança nos sistemas de comunicação e interface de transferência de dados

A princípio os sistemas de comunicação industrial não estavam sujeitos a ataques cibernéticos, uma vez que não existia uma rede de comunicação propriamente dita ou exposição à internet. Os dados ficavam concentrados nos equipamentos e estavam restritos ao ambiente da organização. Entretanto, com a evolução da tecnologia passamos a ter este ambiente de Tecnologia da Operação (TO) e de TI, antes separados, agora em convergência, expostos aos mesmos riscos de ataques.

Como dito anteriormente, é comum encontrarmos no setor elétrico plantas de geração ou de distribuição de energia que estão operando há décadas, pois foram projetadas para ter um tempo de operação longo. Como consequência, diversos IEDs que ainda operam e estão sendo integrados à uma infraestrutura de comunicação mais moderna da empresa, acabam se tornando os elos mais vulneráveis de toda a rede. Esse é um ponto de atenção que deve ser ressaltado para o/a aluno/a. Devido a esta característica do setor elétrico, a principal dificuldade em uma análise de risco é a identificação correta de todos os ativos da empresa, devido a quantidade e tempo de operação destes.

28. Applus Laboratories, "Smart Meter Security Evaluations," Applus Laboratories. Disponível: https://www.appluslaboratories.com/global/en/what-we-do/service-sheet/smart-meters-security-evaluations. [Acesso em 2021 11 14].

Neste contexto, algumas das vulnerabilidades encontradas mais comuns são:

- Protocolos de comunicação de baixa capacidade de segurança;
- Redes de controle sem segmentação, ou seja, sem dispositivos físicos implementados para criar zonas de controle de acesso;
- Redes sem anti-*malwares* ou sem controle de atualizações de *firmwares* dos equipamentos;
- Sistemas operacionais e *firmwares* antigos, sem atualizações e com falhas de segurança conhecidas que podem ser exploradas;
- Sistemas sem registro e controle de acesso ou de incidentes para possibilitar rastreios ou auditorias;
- Sistemas SCADA antigos que dificultam a atualização do próprio sistema ou do equipamento que o comporta.

Ao mesmo tempo que o estabelecimento de protocolos de comunicação no setor elétrico e de automação auxiliaram na integração de dispositivos e, consequentemente, na eficiência dos processos, também expuseram os sistemas às vulnerabilidades conhecidas, uma vez que tais protocolos são conhecidos pelo público e bem documentados.

Inicialmente, os protocolos de comunicação industriais (Modbus, DNP3, etc) foram desenvolvidos para serem utilizados como protocolos de comunicação seriais. Com o passar do tempo e o estabelecimento de outros protocolos de comunicação sobre o TCP/IP, estes protocolos também foram adaptados para essa camada física de operação. Entretanto, essas adaptações não levaram em consideração aspectos de segurança, fazendo com que estes protocolos hoje sejam alvos de ciberataques.

Dica: Estudo sobre uma vulnerabilidade de segurança no protocolo de comunicação GOOSE (IEC 61850-8-1), amplamente utilizado em subestações de energia elétrica que pode ser repassado aos/às alunos/as para prover um exemplo prático.

https://www.nozominetworks.com/blog/iec-61850-meets-iec-62351/

Sistemas SCADA, como visto anteriormente, são utilizados para concentração dos dados de um processo fabril de forma a facilitar o monitoramento, gerenciamento e controle dos processos e dispositivos em campo. O SCADA tem a capacidade de operar com diferentes tipos de protocolos de comunicação industrial. Tais protocolos, como citado acima, apresentam vulnerabilidades que se estendem até o SCADA. Muitos dos ataques cibernéticos ocorridos recentemente no setor elétrico tinham como objetivo obter acesso aos sistemas SCADA. Dessa forma, a seguir são apresentados os objetivos dos criminosos em um ataque dentro deste contexto e quais os prejuízos e possibilidades que incorrem em caso de sucesso do ataque.

Identificar dispositivos que rodam sistemas SCADA e as portas disponibilizadas na rede: uma vez que o cibercriminoso consegue acesso ao sistema, ele pode identificar outros dispositivos com sistemas SCADA e listar portas disponíveis para outros protocolos de comunicação que podem auxiliar a penetrar no restante do sistema. Há portas que são dedicadas (por padrão) para certos protocolos de comunicação ou serviços. Algumas delas são apresentadas na Tabela 3. Dessa forma, ao analisar o sistema o usuário consegue identificar possíveis dispositivos para atacar.

Tabela 3. Portas e serviços conhecidos.

Porta	Serviço
502	Modbus TCP
2222	Ethernet/IP
4840	OPC-UA
20000	DNP3
34962-34964	Profinet
34980	Ethercat

Alterar estado de operação de dispositivos: uma vez que sistemas SCADA podem operar dispositivos de forma remota, o usuário que está atacando a infraestrutura pode alterar o estado de dispositivos críticos, ligando ou desligando, alterando configurações de referência, podendo ocasionar perdas no processo de produção ou até mesmo acidentes.

Ler e escrever informações: através do SCADA o usuário tem a capacidade de ler informações do processo que está sendo gerenciado pelo sistema e alterar informações no banco de dados do SCADA, levando a relatórios de produtividade ou índices de desempenho falsos.

Comprometer outros dispositivos: uma vez que o sistema SCADA possui privilégios de administrador sobre a maioria dos dispositivos que está monitorando ou controlando, fica fácil para o cibercriminoso comprometer outros dispositivos com *malwares*.

Explorar vulnerabilidades: explorar as configurações dos dispositivos, *bugs*, vulnerabilidades na largura de banda da comunicação, entre outros.

Dica: Para protocolos de comunicação industrial, como o Modbus TCP e DNP3, um dos mais utilizados no setor elétrico, há os seguintes materiais que podem ser disponibilizados aos/às alunos/as. Como sugestão, o/a professor/a pode propor a apresentação de seminários para apresentação das principais vulnerabilidades e riscos destes protocolos de comunicação.

Pramod T.C., Sunitha N.R. (2018) “SCADA: Analysis of Attacks on Communication Protocols”. In: Rao N., Brooks R., Wu C. (eds) Proceedings of International Symposium on Sensor Networks, Systems and Security. ISSNSS 2017. Springer, Cham.
https://doi.org/10.1007/978-3-319-75683-7_17

Y. Xu, Y. Yang, T. Li, J. Ju and Q. Wang, "Review on cyber vulnerabilities of communication protocols in industrial control systems," 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), 2017, pp. 1-6, doi: 10.1109/EI2.2017.8245509.

Zurawski, Richard. Industrial Communication Technology Handbook. CRC Press, 2017. Segunda edição. ISBN 9781351831376.

Futuro: Diversas empresas do setor elétrico e de automação, visualizando o crescente número de ataques cibernéticos em infraestruturas críticas, vêm desenvolvendo soluções e dispositivos de segurança para integração a infraestruturas já existentes conforme as boas práticas e normas de cibersegurança. Veja algumas delas que podem ser repassadas aos/às alunos/as:

Schneider: https://www.se.com/ww/en/work/solutions/cybersecurity/industrial-cybersecurity.jsp

Kaspersky Lab: https://www.kaspersky.com.br/enterprise-security/industrial-solution

Siemens: https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security.html

Phoenix Contact: https://www.phoenixcontact.com/pt-pt/produtos/industrial-communication/industrial-routers-and-cybersecurity

2.6. Recapitulando

Ao final deste capítulo, o/a aluno/a deverá ser capaz de:

- Reconhecer vulnerabilidades e ameaças em uma infraestrutura através de metodologias de identificação e reconhecimento;
- Avaliar e estimar os riscos em uma infraestrutura;
- Conhecer os princípios e requisitos mínimos exigidos pela LGPD;
- Propor ações para promoção da ética no tratamento de dados sensíveis no ambiente organizacional;
- Conhecer as normas e padrões internacionais de cibersegurança relacionados ao setor elétrico e de automação (IEEE, ISA, IEC etc.);
- Reconhecer vulnerabilidades em normas e protocolos de comunicação utilizados na indústria do setor elétrico e de automação.

Atividades Sugeridas:

- Apresentações expositivas em slides dos conceitos e definições, por exemplo: das normas de cibersegurança voltadas para o setor elétrico (IEEE, IEC, ISA), tipos de HSM disponíveis no mercado, estudos de caso de análise de vulnerabilidades;
- Apresentação de vídeos para consolidação dos conceitos e para apresentar novidades relacionadas aos temas desta aula, exemplos:
  - https://youtu.be/155yfg0i0iU
  - https://youtu.be/H9y__anQFVw
  - https://youtu.be/oi_CfBe_umU
- Realização de projetos em grupos, por exemplo: fazer uma análise de risco tomando como base o mesmo local para posterior comparação dos resultados entre grupos.

Algumas fontes interessantes:

- https://attack.mitre.org/
- https://www.countercraftsec.com/documents.html
- https://purplesec.us/resources/
- https://cybersecurity.ieee.org/
- **Wilson, Duane C. *Cybersecurity*. MIT Press, 2021. ISBN 9780262365444**
- **Anand Handa; Rohit Negi; Sandeep Kumar Shukla. *Implementing Enterprise Cybersecurity with Open-Source Software and Standard Architecture*. River Publishers, 2021. ISBN 9788770224239**

Avaliação

Apesar de o Brasil ainda não possuir regulamentação específica de cibersegurança para o setor elétrico, o atendimento aos requisitos da LGPD pelas empresas do setor já garante uma robustez ao sistema de segurança da organização. Neste sentido, pesquise sobre quais são os passos para a implementação da LGPD nas empresas e discorra brevemente sobre cada um deles. Além disso, pesquise e liste sobre as principais normas e boas práticas utilizadas pelas empresas do setor elétrico brasileiro.

Capítulo 3: Ações para redução de riscos de ataques virtuais

Nota para o/a professor/a – Como capítulo finalizador, e após o/a aluno/a estar ciente das normas, leis e técnicas para identificar e avaliar riscos de cibersegurança, nesta etapa da disciplina serão abordadas as estratégias para aumento da segurança nas organizações. Essa etapa proporciona ao/à aluno/a conhecimento sobre técnicas para segurança de infraestruturas e procedimentos.

3.1. Aplicações para melhoria de segurança de *hardware* e de infraestrutura

Como já mencionado, a convergência da TO com a TI traz consigo, além dos benefícios, alguns desafios em termos de segurança operacional, uma vez que as soluções tradicionais em sistemas de TI muitas das vezes não se aplicam ou não são adequadas para sistemas de TO.

É muito comum, no setor elétrico, encontrar equipamentos cujos fabricantes não oferecem mais suporte em atualizações de *firmwares*, mas que ainda podem apresentar um longo tempo de utilização pela frente. Cenários como este, com equipamentos com *firmware* defasados, vulnerabilidades conhecidas, protocolos de comunicação proprietários com falhas de segurança etc., apesar de serem comuns, devem ser considerados na mitigação de riscos quando há integração com uma infraestrutura mais moderna de comunicação, a qual expõe os ativos à internet. Neste contexto e diante do que pode ser feito para melhoria da segurança da infraestrutura na empresa, pode-se dividir esse assunto em dois tópicos para melhor entendimento dos/as alunos/as: melhorias de infraestrutura e melhorias de gestão operacional de risco.

Melhorias de infraestrutura

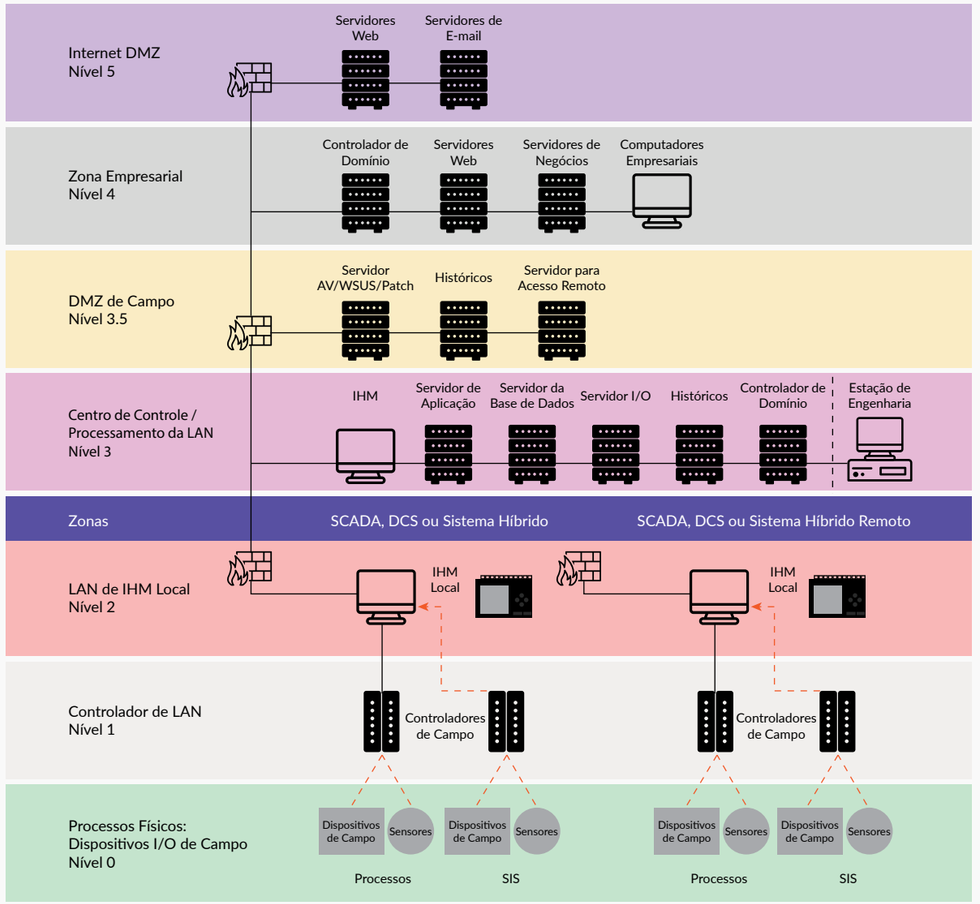
Uma das maneiras mais eficientes de aumentar a segurança da infraestrutura de TO, principalmente em setores como o da energia e automação, é a sua segmentação. Dividir a infraestrutura em segmentos ou zonas de forma que, no caso de um ataque os setores possam ser isolados sem que todo o sistema seja comprometido. A segmentação consiste em separar ativos considerados críticos, adicionando camadas de segurança para controle e monitoramento do tráfego de dados e requisições de acesso.

Para adoção dessa estratégia, é necessário realizar um mapeamento de todos os ativos da empresa e classificá-los conforme sua função e importância dentro do processo de produção. O inventário de ativos deve ser realizado periodicamente e deve conter algumas informações relevantes, tais como:

- Tipo do dispositivo;
- Fabricante do equipamento;
- Responsável pela manutenção e sua função;
- Endereço IP ou MAC *address*;
- Protocolo de aplicação e porta de serviço;
- Versão do *firmware* e/ou sistema operacional quando aplicável.

A arquitetura de referência para segmentação de infraestruturas de TO que é amplamente utilizada é a baseada no modelo de *Purdue* [11] e referenciada na norma ISA95, é dividida em 7 níveis. Cada nível corresponde ao nível e função dos dispositivos no processo produtivo da empresa, desde os dispositivos de campo como sensores, atuadores, motores até os dispositivos de alto nível como servidores de e-mail e internet.

Figura 28. Arquitetura de referência para segmentação de infraestrutura de TO baseada no modelo de Purdue / ISA95[29]



29. Claroty Team, "REVEAL: GAINING VISIBILITY INTO YOUR INDUSTRIAL ENVIRONMENT," Claroty, [Online]. Disponível em: https://claroty.com/2021/04/07/blog-pillars-reveal/. [Acesso em 15 11 2021].

- **Nível 0:** Elementos primários do processo produtivo da empresa tais como sensores, motores, atuadores etc.;
- **Nível 1:** IEDs básicos que fazem interface entre equipamentos do nível 2 e equipamentos do nível 0, e atuam ou monitoram dispositivos do nível 0, como CLPs (Controlador Lógico Programável);
- **Nível 2:** Dispositivos de controle ou monitoramento de área, como IHM (Interface Homem Máquina) e sistemas SCADA;
- **Nível 3:** Sistema de controle do fluxo da operação, que monitoram e intervêm para manter os resultados de produção desejados. Sistemas de aplicação, histórico, base de dados, estação de manutenção local;
- **Nível 3.5:** Seção de autenticação para acesso à infraestrutura de TO. Geralmente são Zonas Desmilitarizadas (DMZ, do inglês *Demilitarized Zone*) que tem como função prover acesso remoto a partir de redes não confiáveis de maneira segura e confiável. Neste nível estão presentes estações de manutenção para acesso remoto;
- **Nível 4:** Nível empresarial onde há aplicações de planejamento e logística, por exemplo;
- **Nível 5:** Infraestrutura de TI da empresa com aplicações para operação da organização como servidores de e-mail e internet.

Saiba mais: DMZs são amplamente utilizadas para acesso remoto de forma segura em uma infraestrutura. Com a especialização das empresas em determinado setor, é comum a contratação de empresas terceirizadas para a manutenção ou aprimoramento, por exemplo, de determinados processos ou infraestruturas. Dessa forma, é essencial fornecer um meio para que usuários externos acessem o sistema de forma segura e controlada.

https://www.fortinet.com/resources/cyberglossary/what-is-dmz

Dica: Há diversos materiais de empresas do setor de cibersegurança que apresentam guias para melhor conduzir a segmentação de uma infraestrutura de TO, que podem ser repassados aos/às alunos/as. Com a convergência de TO com TI fica inevitável a adoção de estratégias para gerenciamento dos ativos de forma segmentada. Abaixo, algumas fontes:

https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-operational-technology-design-guide.pdf

https://www.ge.com/digital/sites/default/files/download_assets/network-segmentation-for-industrial-control-environments-whitepaper.pdf

Melhorias de gestão operacional de risco

Dados os pontos de segurança a serem melhorados em uma infraestrutura, deve-se implementar paralelamente uma metodologia para gestão dos riscos. Considerando o setor elétrico como tema de interesse, podemos adotar as metodologias de gestão voltadas para infraestruturas críticas, conforme apresentado na Figura 29.

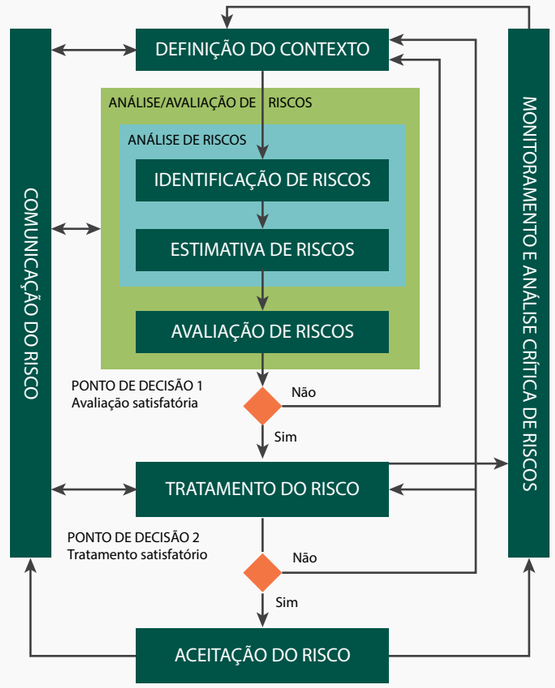
Figura 29. Metodologia para proteção de infraestruturas críticas baseia-se em quatro pilares: prevenção, detecção, resposta e gestão de crises[30]

Metodologia de Proteção de Infraestrutura Crítica

Prevenção	Detecção	Resposta	Gestão de Crises
• Implementar controles de segurança para evitar incidentes de segurança • Uso de metodologias de gestão de riscos	• Monitoramento para identificar situações de segurança • Implantação de Centros de Monitoramento de incidentes	• Identificar, registrar e avaliar incidentes • Informar, avisar e alertar órgãos fiscalizadores • Responder adequadamentea incidentes • Recuperar ambiente operacional	Deve ser parte integrate de uma estratégia de proteção da infraestrutura crítica de informação desde sua concepção

Prevenção: implantação de controles de segurança, políticas de conscientização e informação (erro humano é uma das maiores vulnerabilidades) e análise de riscos (identificação, estimativa e avaliação) conforme ISO/IEC 27005:2008, por exemplo, apresentada na Figura 30.

Figura 30. Processo de gestão do risco conforme ISO/IEC 27005:2008, apresentando as etapas de identificação, estimativa e avaliação de riscos[31]



30. J. R. F. Filho, "Avaliação de Risco e Grau de Maturidade de Cibersegurança para o Setor Elétrico," em Workshop Internacional de Segurança Cibernética, Brasília, 2016.

31. J. H. C. Fernandes, "INTRODUÇÃO À GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO," CEGSIC, Gestão da Segurança da Informação e Comunicações - GSIC, 2011.

Detecção e Resposta: estes pilares se complementam. É necessário implementar meios de monitoramento e detecção de incidentes de segurança e procedimentos para responder a eles. Uma maneira é a implementação de times ou centros de monitoramento e resposta a incidentes que, após a detecção de um incidente, devem responder conforme procedimentos pré-estabelecidos, buscando a contenção de ataques, reestruturação do ambiente atingido, etc. Como exemplo às boas práticas em uma resposta à incidentes é apresentado a Figura 31.

Figura 31. Seis passos para obter uma resposta a incidentes de segurança bem-sucedida[32]

Saiba mais: No Brasil, há um órgão do governo responsável pelo monitoramento, tratamento e resposta a incidentes cibernéticos.
www.gov.br/ctir

Dica: Neste link, o/a aluno/a pode verificar como é realizada a implementação de um programa de gestão de crises:
https://www.rbc.com/cyber-security/_assets-custom/pdf/rbc-cyber-security-crisis-management-template-for-smbs_final_en.pdf

No setor elétrico, considerado uma infraestrutura crítica, há algumas perspectivas e particularidades quando consideramos um programa de gestão de crises, que devem ser repassadas aos/às alunos/as:

https://www2.deloitte.com/hu/en/pages/risk/articles/cyber-crisis-management.html

https://www2.deloitte.com/content/dam/insights/us/articles/4921_Managing-cyber-risk-Electric-energy/DI_Managing-cyber-risk.pdf

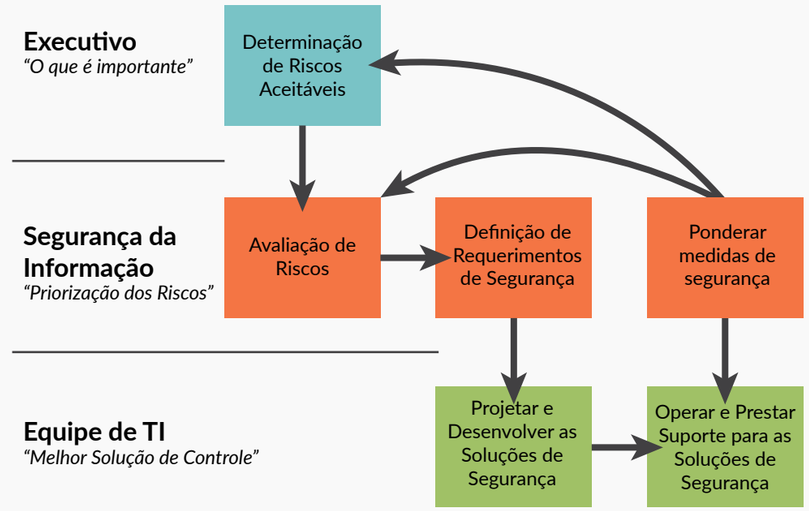
32. Stealth Labs, "The Six Steps to Build an Effective Cyber Incident Response Plan,". Disponível: https://www.stealthlabs.com/blog/the-six-steps-to-build-an-effective-cyber-incident-response-plan/. [Acesso em 15 11 2021].

Como parte fundamental de uma política de gestão de riscos é necessária a formação de uma equipe responsável pelas etapas de prevenção, detecção, resposta e gestão da crise. Além disso, esta equipe é a responsável por realizar as análises de vulnerabilidades e riscos na etapa de prevenção, para implementação de correções e melhorias.

A Figura 32 apresenta um exemplo baseado na metodologia da empresa Microsoft. Neste modelo, os integrantes possuem responsabilidades bem definidas, por exemplo:

- Executivo: pessoa com maior nível hierárquico capaz de avaliar os riscos e vulnerabilidades levantadas em uma análise, ou que surgem durante uma crise, com base nos planos estratégicos da empresa, riscos financeiros e imagem da empresa perante a sociedade;
- Segurança da informação: colaboradores com papel de projetar e gerenciar a estrutura de rede da empresa, fazendo relatórios de análise de riscos e vulnerabilidades. Um nível mais gerencial;
- Grupo de TI: colaboradores que implementam os requisitos repassados pelo pessoal de segurança da informação e presta manutenção à infraestrutura.

Figura 32. Exemplo de atores e suas respectivas funções e responsabilidades em um processo de gerenciamento de risco de segurança, com base na metodologia da empresa Microsoft[33]



Saiba mais: Com o surgimento de novas ameaças e vulnerabilidades, o setor elétrico foi se adaptando e implementando novas estratégias para aumento da segurança em infraestruturas de TO, tais como: segmentação da infraestrutura de TO, detecção e proteção avançada de ameaças, proteção e detecção de ameaças utilizando inteligência artificial, entre outros.
https://www.pwc.com.br/pt/estudos/setores-atividades/energia/2021/Energia%20Cyber_21_VF.pdf
https://www.fortinet.com/content/dam/fortinet/assets/ebook/ebook-advanced-threat-landscape-ot-ciso.pdf

33. DILLARD, K. PFOST, J. , "Security Risk Management Guide," Microsoft Corporation.

3.2. Ações para redução de riscos de cibersegurança

Com a constante evolução dos *softwares* e equipamentos há uma descoberta diária de novas vulnerabilidades, seja devido a um mau desenvolvimento, seja por incompatibilidade de uma atualização de *software* com o *hardware* do dispositivo. Essas novas vulnerabilidades devem ser corrigidas ou mitigadas o quanto antes.

Há uma classe de *softwares*, denominadas *exploits*, que são desenvolvidas com o propósito de se beneficiar de alguma vulnerabilidade em um sistema ou infraestrutura, seja essa vulnerabilidade uma falha de *software*, de *hardware* ou erro humano. Cabe aqui ressaltar que estes *exploits* podem ser utilizados tanto por criminosos que desejam realizar um ataque quanto pela equipe de TI de uma empresa para avaliar suas estratégias de segurança.

Os *exploits* podem ser conhecidos e, portanto, há alguma ferramenta ou maneira de contornar e se proteger deste *exploit*, ou podem ser desconhecidos, também denominados de *zero-day exploits*, que são conhecidos apenas por seus criadores e ainda não foram utilizados. Os desconhecidos reforçam a importância de não considerar apenas o anti-*malware* como uma camada de segurança em uma infraestrutura, pois estes programas operam comparando atividades em um sistema com assinaturas de ameaças já conhecidas.

Ponto de atenção para o/a aluno/a: nem todo *exploit* é um *malware*, mas todo *malware* pode ser considerado um *exploit*. Um *exploit* pode ser um programa que permite um criminoso ter acesso a um computador, por exemplo, para que depois ele instale um *malware*.

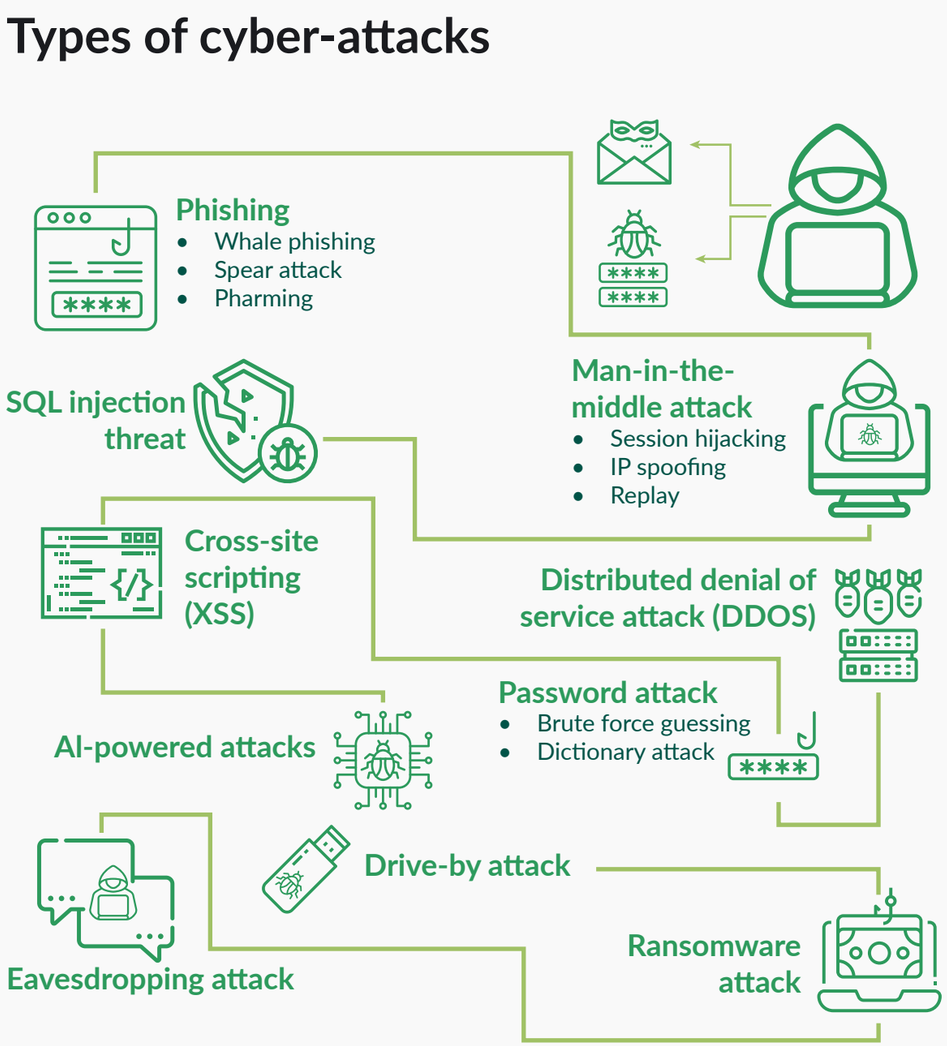
A Figura 33 apresenta os tipos de *exploits* mais utilizados na atualidade. Percebe-se que alguns utilizam *malwares* já mencionados no início deste e-book.

Dica: Os exploits podem se dividir em cinco categorias conforme a característica da vulnerabilidade. São elas: hardware, software, rede, humana e local físico.

https://www.upguard.com/blog/exploit

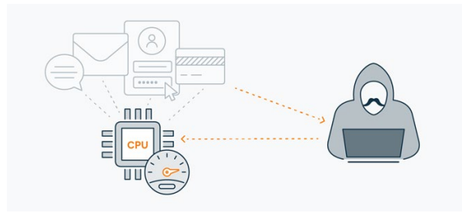
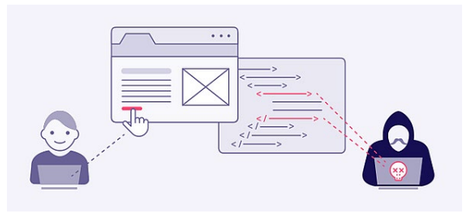
Como sugestão, o/a professor/a pode propor o desenvolvimento de atividades com o objetivo de discentes pesquisarem exploits utilizados no setor elétrico, nestas cinco categorias citadas. Pesquisar quais empresas foram afetadas, quais eram os objetivos, os prejuízos causados, como poderia ter sido prevenido. Como exemplo aos/às alunos/as, o/a professor/a pode apresentar a Tabela 4.

Figura 33. Tipos de exploits mais comuns na atualidade[34].

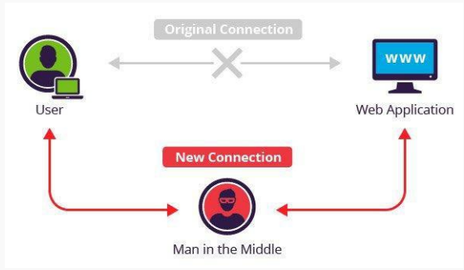


34. Hillary Flyn, "Top Most Common Types Of Cyber Security Attacks," Wellington Management. Disponivel: https://www.wellington.com/en-us/intermediary/insights/esg-cybersecurity-growth-cybercrime-private-companies. [Acesso em 20 07 2022].

Tabela 4. Exemplos de exploits para cada categoria.

EXPLOITS
 35
Tipo | Nome Descrição **Saiba mais: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-exploit.html**
 36
Hardware | Spectre e Metldown Duas vulnerabilidades de *hardwares* presentes em quase todos os dispositivos atualmente (celulares, computadores, tablets etc.) exploradas por *hackers*, possibilitando o roubo de dados privados. **Saiba mais: https://www.avast.com/pt-br/c-meltdown-spectre**
 37
Software | XSS ou Cross-Site Scripting É a injeção de um código malicioso dentro de um site legítimo. O navegador não consegue diferenciar entre o código do site e o código malicioso e acaba por executar o código por completo, acarretando riscos para o usuário, como roubo de dados pessoais. **Saiba mais: https://www.avast.com/c-xss**

35. Fonte: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-exploit.html
36. Fonte: https://www.avast.com/pt-br/c-meltdown-spectre
37. Fonte: https://www.avast.com/c-xss



38

Rede | Man-in-the-Middle

Em uma conexão não segura é possível a interceptação dos dados ou monitoramento por um *hacker*, possibilitando a coleta de dados sensíveis ou manipulação em tempo real.

Saiba mais: https://www.avg.com/pt/signal/man-in-the-middle-attack

39

Local Físico | Controle de acesso

Geralmente facilitado por infraestruturas com baixa ou nenhuma segurança física. O criminoso consegue ter acesso à locais/espaços de uma empresa através da confecção de credenciais ilegais motivadas por baixo nível de segurança das utilizadas pela empresa.

Saiba mais: https://www.upguard.com/blog/access-control

40

Humana | Pishing

É um ataque baseado em estratégias de engenharia social a fim de coletar dados sensíveis como senhas, credenciais etc. Geralmente, inicia-se com um e-mail, com o qual o criminoso se passa por uma organização confiável. O usuário confiando no e-mail é induzido a acessar páginas da internet maliciosas ou instalar programas contendo *malwares*. A partir daí, o criminoso consegue acessar dados da máquina do usuário, ou coletar através de formulários preenchidos pelo próprio usuário.

Saiba mais: https://www.avast.com/pt-br/c-phishing

38. Fonte: https://arkansystem.com.br/blueborne/
39. Fonte: https://www.avg.com/pt/signal/computer-security-exploits
40. Fonte: https://www.avast.com/pt-br/c-phishing

Saiba mais: Todo ataque se inicia com o reconhecimento da empresa e do sistema. Uma estratégia de segurança que pode ser adotada e está ganhando espaço dentre empresas com boas estratégias de cibersegurança, é baseada na enganação (ou *Deception Techniques*) e tem como objetivo detectar o ataque antes que ele aconteça ou durante sua realização.

https://www.countercraftsec.com/downloads/CounterCraft-Anatomy-of-a-cyber-attack.pdf

Considerando as cinco categorias de *exploits*, podemos elencar algumas ações para redução de riscos de cibersegurança.

***Hardware*:** implementar um procedimento de gerenciamento de configurações para que as equipes de TI e TO terão uma visão ampla dos ativos e suas configurações atuais e, com essas informações, tomar decisões de correções, agendar atualizações de *firmware*, solicitar reposição por outro modelo etc.

Saiba mais: Veja em detalhes o que é um gerenciamento de configuração e quais os beneficios:

https://www.upguard.com/blog/5-configuration-management-boss

***Software*:** investir em anti-*malwares*, programas para detecção de vazamentos de credenciais ou dados na internet, política de uso de *softwares* licenciados pela equipe de segurança.

Rede: realizar segmentação da infraestrutura conforme funcionalidade e criticidade dos ativos. Estabelecer regras de *firewall* entre as zonas segmentadas com restrições de portas, protocolos de comunicação, gerenciamento de acessos e requisições de dados. Estabelecimento de critérios mínimos para geração de senhas, utilização de HSM para criptografia de dados e certificados digitais.

Local físico: controle de acesso nos locais via credencial (cartão de acesso) e monitoramento via câmera.

Humana: investimento em educação e informação dos colaboradores da empresa e terceirizados, políticas e práticas de cibersegurança, e treinamento de empresas terceirizadas que tenham atividades em comum com a organização e utilizam da infraestrutura.

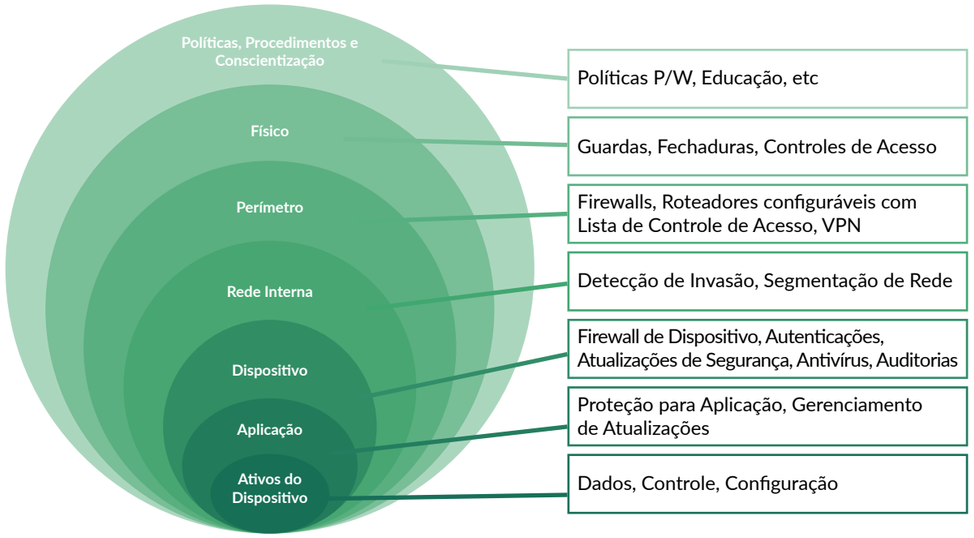
Além disso, a realização de ataques simulados periódicos à própria infraestrutura pela equipe de TI ou TO é altamente recomendável, pois, dessa forma, ficam evidentes vulnerabilidades ou ameaças que passaram despercebidas e há chance de serem corrigidas a tempo. A Figura 34 apresenta alguns passos para guiar a implementação de uma cultura de cibersegurança nas empresas.

Figura 34. Infográfico orientativo sobre como implementar uma cultura de cibersegurança nas empresas[41]

Outra estratégia é a implementação de defesa em profundidade (em inglês, *defense in depth*), a qual tem como objetivo implementar camadas de segurança de forma que haja uma redundância, dificultando que a realização de um ataque consiga atingir os dados mais sensíveis ou ativos mais críticos de uma infraestrutura. A Figura 35 apresenta o conceito de defesa em profundidade e suas camadas.

41. Anchieta Dantas Jr., "Cultura de cibersegurança: como implementar nas empresas," Trendsce. Disponível: https://www.trendsce.com.br/2021/08/04/cultura-de-ciberseguranca-como-implementar-nas-empresas/. [Acesso em 16 11 2021].

Figura 35. Exemplo de camadas de segurança a serem implementadas quando se utiliza da estratégia de defesa em profundidade[42]



Dica: Sugestão de material complementar para os/as alunos/as são estes *guidelines* sobre a implementação de estratégias de defesa em profundidade para o setor elétrico.

https://ieeexplore.ieee.org/document/8274119

https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

3.3. Requisitos e sistemas de monitoramento para inibição da manipulação de dados

A inibição da manipulação de dados é realizada, majoritariamente, pela aplicação do conceito de integridade de dados (em inglês, *data integrity*), que pode ser garantida de várias maneiras. O modelo mais amplamente utilizado na indústria e por pesquisadores é o desenvolvido pelo órgão governamental americano FDA (*Food and Drug Administration*), que contém uma série de princípios. Este modelo é denominado ALCOA, onde as letras de seu nome representam cada princípio a ser seguido. A Figura 36 apresenta cada um dos princípios.

42. Daniel Paillet, "Network Intrusion Detection Systems for Critical Infrastructure," Schneider Electric, 2015.

Figura 36. Princípios do modelo ALCOA para garantia da integridade dos dados e consequente coibição da manipulação de dados.43

ATRIBUÍVEL
O dado gerado ou coletado deve estar atribuído a quem realizou a ação e quando a ação foi realizada.
Essa atribuição pode ser feita manualmente, através de uma assinatura e data ou eletronicamente por Audit Trail.

LEGÍVEL
O dado coletado ou gerado deve ser registrado de forma legível e permanente.

CONTEMPORÂNEO
O dado deve ser registrado no momento em que a ação ocorre.

ORIGINAL
O dado deve ser anotado diretamente no Log Book oficial da empresa, evitando anotações provisórias e posterior transcrição desses dados.

ACURADO
O dado gerado deve ser livre de erros, completo e verdadeiro, refletindo exatamente as ações determinadas no processo produtivo.

Estes princípios podem ser alcançados de diversas maneiras. A implementação de um sistema que identifica um dado a uma fonte, pessoa ou processo de forma automática consegue atender ao requisito de "Atribuível".

Já para ser "Legível" os dados precisam conseguir ser lidos. A maioria dos dados armazenados eletronicamente garantem isso, porém há aqueles dados sensíveis que são obtidos através de digitalização de documentos, por exemplo. Nestes casos, a adoção de normas pré-estabelecidas para estes procedimentos deve garantir uma padronização de documentos obtidos desta forma.

Juntamente com o sistema automatizado sugerido para o princípio "Atribuível", há a possibilidade de incluir uma automatização para inserção de "*time stamps*" (registro de tempo) a cada criação, modificação, transferência ou exclusão de um dado. Dessa forma, garante-se o princípio "Contemporâneo".

Para atendimento ao princípio "Original", o dado deve, no momento de sua coleta ou criação, carregar consigo um registro de data, assinatura eletrônica do responsável pela inserção do dado no sistema e metadados relevantes. Estas informações originais devem ser mantidas no registro de dados independente da necessidade de anotações nestes dados ou modificações diversas.

Por fim, um sistema automatizado de coleta de dados sem interferência humana deve satisfazer o princípio de "Acurado", ou seja, livre de erros e completo.

A Figura 37 apresenta algumas das ações adicionais que podem ser tomadas para garantia da integridade dos dados.

43. F. Q. Demetrius Rocha, "Data Integrity na indústria farmacêutica," BOAS PRÁTICAS. Disponível: http://boaspraticasnet.com.br/data-integrity-na-industria-farmaceutica/. [Acesso em 16 11 2021].

Figura 37. Algumas das ações que podem ser tomadas para preservar a integridade dos dados[44]

Com a digitalização do setor elétrico, introdução de tecnologias IoT como Wi-Fi, GPS *tracking* ou RFID (do inglês, *Radio-Frequency Identification*) nas infraestruturas das organizações e nas casas de clientes para oferta de novos serviços (como é o caso do *smart meter*), há a necessidade de considerar medidas de segurança também pelo lado do cliente e de empresas terceiras. Por esse motivo, a garantia de uma linha de comunicação segura entre a origem do dado e o ponto de coleta também é de extrema importância na integridade dos dados. Isso previne ataques de *exploits* como o *Man-in-the-Middle,* por exemplo.

Dica: Como sugestão, o/a professor/a pode propor a realização de atividades como seminários, com o objetivo de os/as alunos/as trazerem exemplos de estratégias de preservação da integridade dos dados implementadas por empresas do setor elétrico.

44. CINDY NG, "What is Data Integrity?," Varonis. Disponível: https://www.varonis.com/blog/data-integrity/. [Acesso em 16 11 2021].

Saiba mais: Um dos tipos de ataques mais executados hoje em dia e que comprometem a integridade dos dados são ataques por ransomware, onde o programa faz a criptografia dos dados do sistema infectado de forma a impedir que estes sejam acessados. A liberação só é feita mediante pagamento de um resgate, geralmente.

O Instituto Nacional de Padrões e Tecnologia (do inglês, *National Institute of Standards and Technology* – NIST), visando essa tendência nos ciberataques, elaborou um guia com práticas para recuperação dos dados diante destes cenários que pode servir de material complementar aos/às alunos/as:

https://www.nccoe.nist.gov/data-integrity-recovering-ransomware-and-other-destructive-events

3.4. Recapitulando

Ao final deste capítulo, o/a aluno/a deverá ser capaz de:

- Reconhecer e propor pontos de melhoria de cibersegurança em uma infraestrutura de operação;
- Propor ações para redução de risco de ataques por *exploits* baseado em sua classificação;
- Recomendar programas e políticas de cibersegurança no ambiente profissional, especialmente no setor elétrico: pessoas, processos e tecnologia;
- Identificar processos que possam afetar a integridade de dados.

Atividades Sugeridas:

- Apresentações expositivas em slides dos conceitos e definições, por exemplo: segmentação de infraestrutura de TO utilizando um caso real, expondo em detalhes os procedimentos de uma gestão de risco, exemplos de *exploits*;
- Apresentação de vídeos para consolidação dos conceitos e para apresentar novidades relacionadas aos temas desta aula, exemplos:
  - https://youtu.be/vSHrZx5HmBw
  - https://www.youtube.com/watch?v=K3CTAHT3WxQ
  - https://www.youtube.com/watch?v=OBEfA4DdcT0
- Promover atividades em grupo e individuais, tais como seminários, para avaliação do aprendizado: estudo de caso de segmentação de TO, de programas de promoção de cibersegurança, explanação detalhada de normas relevantes como IEEE, IEC e ISA.

Algumas fontes interessantes:

- https://www.fortinet.com/
- https://claroty.com/
- https://www.enisa.europa.eu/topics/cyber-crisis-management?tab=publications
- https://www.upguard.com/resources
- Howard Shrobe; David L. Shrier; Alex Pentland. *New Solutions for Cybersecurity*. MIT Press, 2018. ISBN 9780262346641
- Feng Ye; Yi Qian; Rose Qingyang Hu. *Smart Grid Communication Infrastructures: Big Data, Cloud Computing, and Security*. Wiley-IEEE Press, 2017. ISBN 9781119240150
- Mariana Hentea. *Building an Effective Security Program for Distributed Energy Resources and Systems*. Wiley Telecom, 2021. ISBN 9781118949047

Avaliação

Considerando a Figura 38 e as estratégias para implementações de melhorias de segurança em infraestrutura de TO apresentadas neste capítulo, proponha adequações à estrutura de forma a seguir as recomendações do modelo de *Purdue*.

Figura 38. Diagrama simplificado de uma infraestrutura de TO[45]

45. P. R. A. d. S. Junior, "Segurança cibernética para sistemas de automação de energia," em Workshop Internacional de Segurança Cibernética, 2016.

Atividades Sugeridas

- Apresentações de convidados/as externos/as que possuem conhecimento de mercado e poderá trazer bons exemplos de aplicações;
- Dinâmicas de grupo para discussão, solidificação dos conceitos e troca de informações sobre as diversas aplicações;
- Enviar artigos científicos de congressos e periódicos para consolidação dos conceitos e apresentação de estudos no estado da arte;
- Indicar links de sites de notícias com conceitos, definições e notícias mais recentes sobre a evolução das tecnologias;
- Indicar links de documentos, tais como relatórios e estudos de agências, institutos de pesquisa e órgãos governamentais relacionados aos temas e novidades no âmbito regulatório;
- Indicar links de redes sociais de pessoas com alto conhecimento na área e no tema para tomada de subsídios para novos projetos;
- Convidar os/as alunos/as para participarem de webinar e outros eventos disponibilizados pela instituição como forma de intensificar essa capacitação.

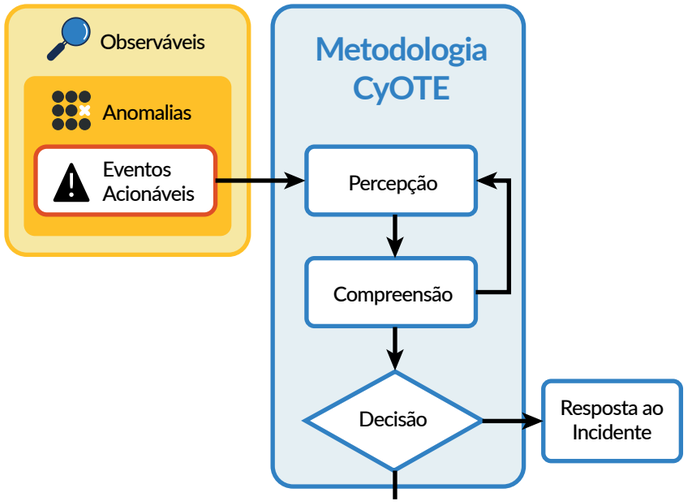
Casos de sucesso

Caso 1: CyOTE - Cybersecurity for the Operational Technology Environment.

Local: Estados Unidos
Descrição: A iniciativa CyOTE é um investimento de alta prioridade do Departamento de Energia dos Estados Unidos (do inglês *Department of Energy* – DOE) para aprimorar a detecção de ameaças no setor de energia de comportamento anômalo potencialmente indicando atividade cibernética maliciosa em redes de Tecnologia da Operação (TO).

A CyOTE criou um método de detecção de ameaças cibernéticas para que as empresas do setor de energia identifiquem de forma independente as técnicas adversárias em seus ambientes de TO que podem resultar em interrupções físicas nos fluxos de energia ou danos a equipamentos. Essa metodologia é única porque vincula as informações das operações a partir da percepção inicial de um evento desencadeador e permite que proprietários e operadores compreendam as informações e tomem decisões mais rápidas e com maior confiança.

Figura 39. Metodologia do CyOTE[46]



Saiba mais: Veja mais sobre a iniciativa CyOTE:
https://inl.gov/wp-content/uploads/2021/09/CyOTE-Methodology_2021.pdf

46. Fonte: https://inl.gov/cyote/

Caso 2: Threat Response and Analysis Center (TRAC) – Dominion Energy.

Local: Estados Unidos
Descrição: A Dominion Energy é uma grande empresa de energia dos Estados Unidos, que atua no fornecimento de gás e energia elétrica para mais de cinco milhões de unidades consumidoras em 18 estados. A empresa é um ativo nacional crítico (fornece energia para o Pentágono e outras grandes e críticas unidades consumidoras) e por isso é alvo constante de ataques cibernéticos.

Uma das estratégias adotadas pela Dominion no quesito de cibersegurança foi a criação do Centro de Análise e Resposta de Ameaças (do inglês *Threat Response and Analysis Center* – TRAC). O TRAC é uma organização de segurança integrada que fornece à alta liderança e todas as camadas hierárquicas da Dominion informações para tomar decisões estratégicas que mitigam os riscos e fornecem uma resposta oportuna e coordenada às ameaças táticas que surgem.

Recomendações da Dominion Energy para cibersegurança em empresas de energia:

Desenvolva inteligência estratégica de ameaças que seja relevante para o C-Level:

- Gere relatórios de inteligência com o impacto potencial das ameaças nos negócios.
- Integre relatórios de inteligência ao planejamento estratégico.
- Elabore planos de resposta a incidentes com clareza de processos.

Integre a segurança em todas as regiões onde empresa atua em áreas e departamentos:

- Centralize todas as regiões e unidades de negócios sob um único conjunto de padrões de segurança cibernética com informações de toda a empresa.
- Crie um quadro operacional comum para segurança física, cibersegurança e TI.
- Integre a segurança à cultura das unidades de negócios.
- Crie processos estruturados para compartilhamento de informações relacionadas à segurança e tomada de decisões nas organizações.
- Projete DMZs claras e seguras entre a rede de TI e TO de acordo com um conjunto definido de regras.
- Identifique e crie zonas de segurança para proteger criticidades nas redes de TI e TO.

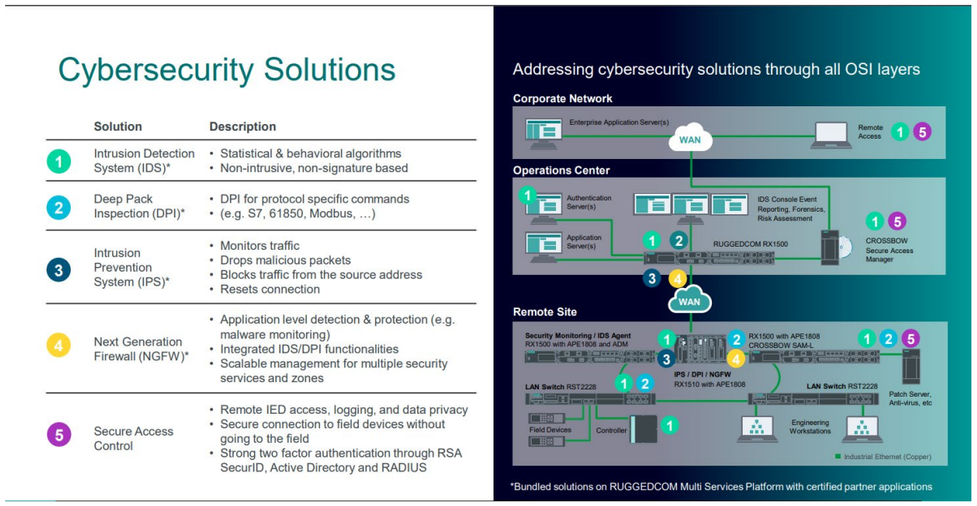
Saiba mais: Veja mais sobre a iniciativa da Dominion Energy:
https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities

Caso 3: Siemens – Cibersegurança em subestações digitais.

Descrição: Uma das grandes preocupações de cibersegurança no setor elétrico é o potencial de ataque cibernético a subestações. Dessa forma, na medida em que fornecedores passam a oferecer soluções de subestações automatizadas/inteligentes/conectadas, surge cada vez mais a necessidade de modernização nas condições de cibersegurança desses sistemas.

Nesse cenário, a Siemens desenvolveu um conjunto de medidas de segurança cibernética apropriadas para serem aplicadas sistematicamente durante a engenharia da subestação, incluindo reforço do sistema, proteção contra malware e controle de acesso. O padrão internacional IEC é projetado para verificar a eficácia das medidas de segurança cibernética na integração do sistema e o conceito de subestação segura da Siemens é certificado por organismos internacionais.

Figura 40. Medidas de Cibersegurança em subestações digitais[47]



Saiba mais: Veja mais sobre soluções de cibersegurança da Siemens para setor de energia:
https://new.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/grid-security.html

47. Fonte: https://assets.new.siemens.com/siemens/assets/api/uuid:6d8d8d9b-d5db-4540-9b5f-6fd6e9ecefac/di-pa-ci-digital-substation-ipdf-en.pdf

Entidades a consultar sobre o tema de cibersegurança

Aqui são apresentadas algumas entidades relevantes para consultas sobre o tema de cibersegurança, onde é possível encontrar mais informações técnicas, estudos de casos, tendências, referências e padrões e rede de indústrias e instituições envolvidas no tema.

NCCoE – National Cybersecurity Center of Excellence (Estados Unidos)

https://www.nccoe.nist.gov/

Atuação:

- Reúne especialistas da indústria, governo e academia para atender às necessidades do mundo real de segurança de sistemas de TI complexos e proteção da infraestrutura crítica dos EUA.
- Gera especificações técnicas de problemas e mapeia a solução desejada para o NIST (*National Institute of Standards and Technology* – Instituto Nacional de Padrões e Tecnologia), define padrões e identifica melhores práticas da indústria.
- Agrega fornecedores de tecnologias para a cibersegurança.

Por que consultar: A NCCoE, como iniciativa vinculada ao NIST, é referência no que se refere a padronização e recomendações de boas práticas de cibersegurança. Desde 2013, a NCCoE tem fornecido orientação e soluções de exemplo para ajudar concessionárias e operadoras de infraestrutura crítica de energia elétrica a proteger os complexos sistemas de TI e Tecnologia da Operação (TO) do setor.

CESER – Cybersecurity, Energy Security, and Emergency Response (Estados Unidos)

https://www.energy.gov/ceser/office-cybersecurity-energy-security-and-emergency-response

Atuação:

- CESER é um órgão vinculado ao DOE (Departamento de Energia dos Estados Unidos), cujo foco são atividades de preparação, antecipação e resposta a ameaças cibernéticas, visando a segurança para o país.
- Atua em parceria com centros de pesquisa no país para testar componentes e configurações com base no *feedback* da indústria, por meio de um programa específico, o Programa de Compartilhamento de Informações de Risco de Segurança Cibernética.
- As ações do CESER de detecção e resposta a ataques cibernéticos são realizadas em estreita interação com órgãos do governo e as empresas do setor de energia, sendo o responsável pela coordenação de ações.

Por que consultar: Por meio do CESER é possível acessar a informações sobre tecnologias e abordagens para cibersegurança no estado da arte, bem como ferramentas de modelagem e solução de problemas desenvolvidas e disponibilizadas pelo DOE.

ONS – Operador Nacional do Sistema Elétrico (Brasil)

http://www.ons.org.br/

Atuação:

- O ONS é o órgão responsável pela coordenação e controle da operação das instalações de geração e transmissão de energia elétrica no Sistema Interligado Nacional (SIN) e pelo planejamento da operação dos sistemas isolados do país, sob a fiscalização e regulação da Agência Nacional de Energia Elétrica (ANEEL).
- Tem como objetivos principais: (a) promover a otimização da operação do sistema eletroenergético, visando ao menor custo para o sistema, observados os padrões técnicos e os critérios de confiabilidade estabelecidos nos Procedimentos de Rede aprovados pela ANEEL; (b) garantir que todos os agentes do setor elétrico tenham acesso à rede de transmissão de forma não discriminatória; e (c) contribuir, de acordo com a natureza de suas atividades, para que a expansão do SIN se faça ao menor custo e vise às melhores condições operacionais futuras.
- No que se refere ao tema de cibersegurança, o ONS, junto à ANEEL, aprovou em 14 de dezembro de 2021 a regulamentação sobre segurança cibernética no setor elétrico. No entanto, uma interação entre os dois órgãos implantou em julho de 2021 uma rotina operacional estabelecendo os requisitos mínimos de segurança cibernética para o setor elétrico.

Por que consultar: O ONS é o órgão que está liderando a estruturação de políticas e práticas para segurança cibernética no setor elétrico brasileiro. Por meio do ONS é possível obter informações atualizadas e ao mesmo tempo contribuir com a construção deste tema no país.

BSI – Federal Office for Information Security (Alemanha)

Bundesamt für Sicherheit in der Informationstechnik

https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

Atuação:

- Investiga riscos de segurança associados ao uso de sistemas de TI e desenvolve soluções para prevenção de ataques e melhoria da segurança.
- Fornece relatórios e informações sobre riscos e ameaças atuais do mercado nacional e internacional.
- Fornece consultoria (testes de segurança e desenvolvimento de soluções) para empresas terceiras privadas ou governamentais.
- Desenvolve normas e guias de boas práticas para a indústria.

Por que consultar: O BSI é o órgão governamental responsável pela normatização referente à cibersegurança no país. Além disso, oferece serviços de consultoria para empresas privadas e outros órgãos governamentais através de sua estrutura organizacional dividida em 7 setores especializados.

Fechamento

O setor elétrico conta com complexos desafios pela frente para garantia da cibersegurança em suas infraestruturas operacionais. Isso se deve, principalmente, à forma como vem ocorrendo a digitalização deste setor. O conhecimento dos conceitos de cibersegurança, seus respectivos protocolos e processos, padrões e sistemas são essenciais para uma visão sistêmica dos riscos.

Diversas usinas de geração de energia, distribuição ou centros de automação, por exemplo, geralmente são projetados e construídos de forma que tenham um ciclo de vida de operação longo, de 15 a 20 anos. Neste sentido, equipamentos antigos que ainda operam nos dias de hoje são incluídos na infraestrutura de comunicação das empresas a fim de que os operadores tenham um sistema automatizado fornecendo maior controle e supervisão dos processos. Entretanto, tais equipamentos, muitas das vezes, não possuem mais suporte por parte do fabricante para atualização de *software* ou *firmware*, como por exemplo correções de segurança de vulnerabilidades já conhecidas, fazendo com que estes dispositivos se tornem o elo fraco em uma infraestrutura crítica.

Por isso é importante que sejam avaliados todos os riscos de segurança aos quais os sistemas elétricos estão sujeitos. Entender como estes riscos podem ser mitigados requer um conhecimento intenso nas matérias do setor elétrico, mas também nas matérias sobre sistemas computacionais. Com isso o profissional poderá criar soluções para evitar que suas instalações fiquem vulneráveis.

Neste sentido, o profissional do futuro do setor elétrico deve estar sempre atualizado e com as ferramentas adequadas para analisar, reconhecer e aplicar ações no sentido de evitar riscos e vulnerabilidades nos sistemas de controle e operação das redes elétricas atuais e do futuro.

É nesse sentido que esse e-book se mostra importante ao compilar os conteúdos mais relevantes a serem passados por docentes a alunos e alunas de disciplinas relacionadas à cibersegurança. Espera-se que, com disciplinas atualizadas, estudantes de cursos que têm interação com o setor elétrico finalizem seus cursos com conhecimentos mais aderentes aos exigidos pelo atual mercado de trabalho.

Glossário

ANEEL	Agência Nacional de Energia Elétrica
ANATEL	Agência Nacional de Telecomunicações
CLP	Controlador Lógico Programável
CPS	*Cyber-Physical System* (Sistema Cibernético-Físico)
DDoS	*Distributed Denial of Service* (Ataque de Negação de Serviço)
DMZ	*Demilitarized Zone* (Zona Desmilitarizada)
DOE	*Department of Energy* (Departamento de Energia)
EMS	*Energy Management System* (Sistema de Gerenciamento de Energia)
EULA	*End-User License Agreement* (Acordo de Licença de Usuário Final)
FDA	*Food and Drug Administration*
GDPR	*General Data Protection Regulation* (Regulamento Geral sobre a Proteção de Dados)
GESEL	Grupo de Estudos do Setor Elétrico
HSM	*Hardware Security Module* (Módulo de Segurança de Hardware)
IA	Inteligência Artificial
IEC	*International Electrotechnical Commission* (Comissão Eletrotécnica Internacional)
IEDs	*Intelligent Electronic Devices* (Dispositivos Eletrônicos Inteligentes)
IHM	Interface Homem Máquina
IIoT	*Industrial Internet of Things* (Internet Industrial das Coisas)
IoE	*Internet of Energy* (Internet da Energia)
IoT	*Internet of Things* (Internet das Coisas)
LGPD	Lei Geral de Proteção de Dados
NIST	*National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia)
NREL	*National Renewable Energy Laboratory* (Laboratório Nacional de Energia Renovável)
ONS	Operador Nacional do Sistema Elétrico
RFID	*Radio-Frequency Identification* (Identificação por Radiofrequência)
SAGE	Sistema Aberto de Gerenciamento de Energia
SCADA	*Supervisory Control And Data Acquisition* (Sistema de Supervisão e Aquisição de Dados)
SIN	Sistema Interligado Nacional
TI	Tecnologia da Informação
TO	Tecnologia da Operação
TRAC	*Threat Response and Analysis Center* (Centro de Análise e Resposta de Ameaças)
VPN	*Virtual Private Network* (Rede Privada Virtual)

Referências

[1] CISO Advisor, "Baixo investimento ajudou sucesso de ataques no Brasil, mostra pesquisa," CISO Advisor, [Online]. Available: https://www.cisoadvisor.com.br/baixo-investimento-ajudou-sucesso-de-ataques-no-brasil-mostra-pesquisa/. [Acesso em 11 12 2021].

[2] Ana Luiza Mahlmeister, "Maior vulnerabilidade a ataques está nas pessoas," Valor Globo, [Online]. Available: https://valor.globo.com/brasil/noticia/2021/10/28/maior-vulnerabilidade-a-ataques-esta-nas-pessoas.ghtml. [Acesso em 17 11 2021].

[3] NSFOCUS, "2020 Cybersecurity Insights Report," [Online]. Available: https://nsfocusglobal.com/pt-br/company-overview/resources/2020-cybersecurity-insights-report/.

[4] IEC, "IEC 61850 - Communication networks and systems for power utility automation," IEC, 2003.

[5] H. Shahinzadeh, J. Moradi, G. B. Gharehpetian, H. Nafisi and M. Abedi, "Internet of Energy (IoE) in Smart Power Systems," *2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI),* pp. 627-636, 2019.

[6] Eletrobras, Cepel, "SAGE - Sistema Aberto de Gerenciamento de Energia," [Online]. Available: http://www.cepel.br/pt_br/produtos/sage-sistema-aberto-de-gerenciamento-de-energia.htm. [Acesso em 09 2021].

[7] David Kim, Michael G. Solomon, Fundamentals of Information Systems Security, Jones & Bartlett Learning, 2018.

[8] J. H. C. Fernandes, "INTRODUÇÃO À GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO," CEGSIC, Gestão da Segurança da Informação e Comunicações - GSIC, 2011.

[9] Bruno Mattiuzo, "O retorno sobre o investimento em cibersegurança," RedBelt, [Online]. Available: https://www.redbelt.com.br/blog/2021/06/24/o-retorno-sobre-o-investimento-em-ciberseguranca/. [Acesso em 12 01 2022].

[10] *ISO/IEC FDIS 27005 - Information technology - Security Techniques - Information,* 2018.

[11] ZScaler, "What is the Purdue Model for ICS security?," [Online]. Available: https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security. [Acesso em 13 01 2022].

Respostas das Avaliações

Capítulo 1

A acessibilidade à sistemas fotovoltaicos por parte dos consumidores de energia elétrica, a modernização dos sistemas de leitura de energia para geração das faturas por parte das concessionárias, a utilização de equipamentos e dispositivos de forma integrada (IoT) por parte do consumidor são exemplos que destacam a participação do cliente/consumidor indiretamente em parte do sistema de comunicação de uma empresa de energia elétrica.

A digitalização do setor elétrico obviamente trouxe benefícios e permitiu a oferta de novos serviços aos clientes, porém a necessidade dessa interação da empresa com o cliente através de redes de comunicação adiciona uma vulnerabilidade na infraestrutura da organização, uma vez que o cliente não terá a mesma capacidade de proteção ou procedimentos de cibersegurança em sua casa.

Capítulo 2

Há diversas fontes na internet com sugestões sobre quais são os passos para que uma empresa implante ou se adeque aos requisitos da LGPD. Portanto, de forma sucinta, a seguir estão os passos:

1. Estudo da LGPD e demais leis relacionadas: A equipe que será responsável pela implementação da LGPD deve estudar a lei em sua plenitude e demais leis relacionadas.
2. Mapear a entrada e o tratamento dos dados sensíveis.
3. Elaboração de relatório de impacto conforme previsto no artigo 5º, inciso XVII da LGPD.
4. Criar política de proteção de dados.
5. Gerenciar os pedidos dos titulares e dos órgãos, tais como solicitação de exclusão, alteração de consentimento, pedido de auditoria, etc.
6. Treinamento das equipes envolvidas na operação de dados pessoais conforme política de proteção de dados e regras de boas práticas e de governança.
7. Ser *compliance* com a proteção de dados mediante política de proteção de dados e governança e exigir de fornecedores e demais relacionados o mesmo *compliance*.
8. Eleger um Encarregado da Proteção de Dados (do inglês *Data Protection Officer* – DPO).
9. Por fim, certificar a empresa através de uma auditoria especializada nas práticas relacionadas à LGPD.

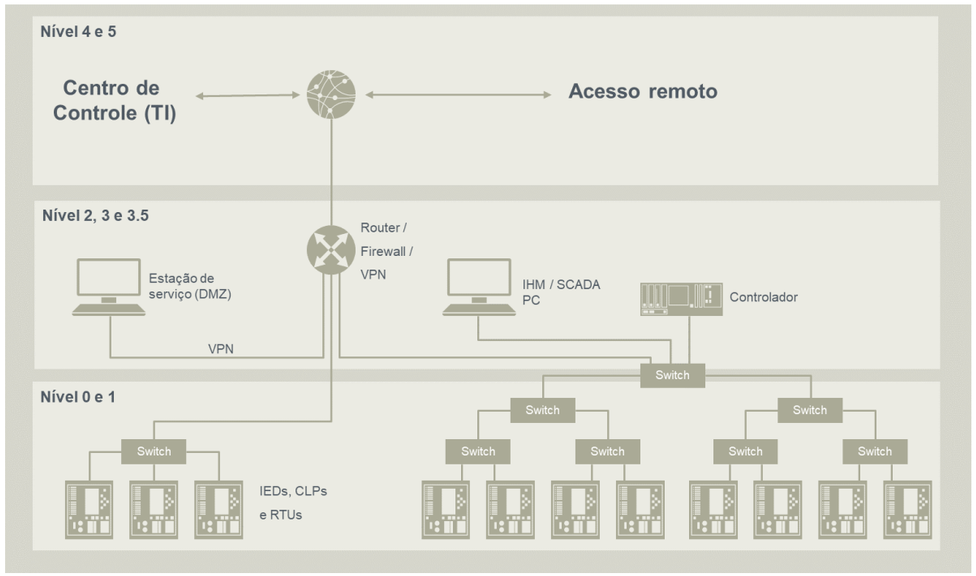
Capítulo 3

Conforme o modelo de *Purdue* referenciado na norma ISA95, é recomendado que em infraestruturas de TO seja feita a segmentação de forma que os dispositivos que as compõem sejam divididos conforme sua funcionalidade e criticidade para o processo da empresa.

A Figura 38 apresenta uma topologia de infraestrutura denominada linear ou barramento único, onde todos os dispositivos estão conectados à um único barramento de comunicação sem segmentação alguma através de dispositivos que possibilitem um controle de tráfego ou controle de acessos.

Portanto as sugestões para melhoria desta infraestrutura devem seguir o apresentado na Figura 41 onde é feita a segmentação dos dispositivos conforme os níveis do modelo de *Purdue*. Estes dispositivos (*switches, routers*) permitem a implementação de *firewalls*, controle de acesso, restrição de protocolos de comunicação e monitoramento do tráfego. Além disso, o acesso remoto é feito através de uma estação DMZ para garantir acesso seguro e confiável de usuários externos à intranet da empresa.

Figura 41. Diagrama simplificado da infraestrutura de TO conforme recomendações de cibersegurança seguindo o modelo de Purdue[48].



48. P. R. A. d. S. Junior, "Segurança cibernética para sistemas de automação de energia," em Workshop Internacional de Segurança Cibernética, 2016.

Este ebook faz parte de uma coleção de quatro apostilas desenvolvidas pelo projeto Profissionais do Futuro: Competências para a Economia Verde.

Confira abaixo os demais exemplares:

Sistemas de armazenamento de energia

Machine Learning e Big Data no Setor Elétrico

Recursos Energéticos Distribuídos e Redes Elétricas Inteligentes

cooperação alemã
DEUTSCHE ZUSAMMENARBEIT

Por meio da:

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Profissionais do Futuro

MINISTÉRIO DA EDUCAÇÃO

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO