CIBERSEGURANÇA EM REDES DE DADOS DE AUTOMAÇÃO – DESAFIOS E MITIGAÇÃO DE RISCOS CONFORME NORMA ISA/IEC 62443

Anderson Augusto Serodio
Engenheiro Eletricista (2008) pela Escola Politécnica da Universidade de São Paulo. MBA em Automação Industrial pelo PECE-Poli-USP (2019). Engenheiro da SABESP - Companhia de Saneamento Básico do Estado de São Paulo desde 2012. Tel: +55 (11) 3386-9820 - e-mail: aserodio@sabesp.com.br.
Marcelo Tadeu da Silva Pereira
Bacharel em Ciência da Computação (2001). MBA em Automação Industrial pelo PECE-Poli-USP (2020). Técnico em Gestão e Coordenador de Projetos Estratégicos de TI na SABESP - Companhia de Saneamento Básico do Estado de São Paulo. Diretor da ISA São Paulo Section. Tel: +55 (11) 95602-3576 - e-mail: mtspereira@sabesp.com.br.

Endereço: Rua Costa Carvalho, 300 – Pinheiros – São Paulo – SP – CEP: 05429-900 – Brasil – Tel: +55 (11) 3386-9820 - e-mail: aserodio@sabesp.com.br.

RESUMO

O ambiente com as redes de TI (Tecnologia da Informação) e TO (Tecnologia Operacional) integradas estabelece as condições perfeitas para um ataque cibernético, pois as redes de automação têm pouca maturidade em relação aos controles de segurança cibernética, uma vez que foram originalmente concebidas com a suposição de que não estariam expostas às ameaças. Além da questão de maturidade, as estratégias de segurança para redes de TI diferem das estratégias de segurança para redes de TO. Enquanto a proteção de dados é prioridade em TI, em TO o foco principal é a continuidade do processo e a preservação de vidas e do meio ambiente. Neste sentido, o presente trabalho busca descrever conceitos importantes sobre a cibersegurança em redes de dados de automação, identificar ameaças e vulnerabilidades aos quais as redes de automação estão susceptíveis e propor ações para mitigação dos riscos, usando como pano de fundo a norma ISA/IEC 62443.

PALAVRAS-CHAVE: cibersegurança, rede de dados de automação, norma ISA/IEC 62443.

1. INTRODUÇÃO

Historicamente, a automação teve início por meio de automações isoladas, conhecidas como “ilhas de automação”. Tais projetos visavam controlar uma instalação operacional específica ou processos específicos dentro de uma instalação operacional, sem qualquer comunicação com redes de dados e o restante da empresa.

Com o avanço tecnológico e a redução dos custos de implantação, tornou-se propício às empresas automatizar em larga escala seus sistemas e instalações operacionais. Atualmente, cada vez mais, as instalações e sistemas industriais dependem da automação para sua operação e gestão. Como consequência, o avanço tecnológico permitiu a integração das “ilhas de automação” às outras redes da empresa, integrando o chão de fábrica com a rede corporativa. Em outras palavras, as redes de automação começaram a se conectar com as redes de TI, abrindo caminho para integrações com a própria *internet*. Essa automação trouxe benefícios, como gestão mais eficaz, facilidade do acesso à informação e otimização do tempo e da mão-de-obra. Porém, esse movimento convergente que integrou as redes de TI (Tecnologia da Informação) e TO (Tecnologia Operacional) em uma única rede, apesar de benéfico, se tornou um grande problema de segurança cibernética.

O ambiente com as redes de TI e TO integradas estabelece as condições perfeitas para um ataque cibernético, pois as redes de automação têm pouca maturidade em relação aos controles de segurança cibernética, uma vez que foram originalmente concebidas com a suposição de que não estariam expostas às ameaças. Além da questão de maturidade, as estratégias de segurança para redes de TI diferem das estratégias de segurança para redes de TO. Enquanto a proteção de dados é prioridade em TI, em TO o foco principal é a continuidade do processo e a preservação de vidas e do meio ambiente.

Desta forma, uma solução para redes de TI, incluindo a cibersegurança de TI clássica, geralmente é inadequada para uso em redes de TO, podendo colocar a disponibilidade, a integridade e a segurança dos processos em risco.

Neste contexto, faz-se necessário entender os desafios de segurança cibernética em redes de dados de sistemas de controle e automação industrial, principalmente de infraestruturas críticas, e encontrar soluções para mitigação dos riscos, eliminação das vulnerabilidades e proteção contra ameaças.

Como referência temos a série de normas ISA/IEC 62443, que define os métodos de proteção para sistemas de controle e automação. A norma ISA/IEC 62443 é composta por um conjunto de documentos com o objetivo de auxiliar na operação segura de sistemas de automação, contemplando desde o design, passando pela implementação, até o gerenciamento das redes de TO.

2. OBJETIVOS

O principal objetivo deste trabalho é apresentar os desafios de cibersegurança em redes de automação, num cenário de convergência de redes de TI e TO, e propor ações para mitigação de riscos, utilizando como referência a série de normas ISA/IEC 62443.

3. METODOLOGIA UTILIZADA

Para o desenvolvimento deste artigo foi adotada a abordagem descritiva associada à pesquisa bibliográfica, baseada em artigos técnicos e acadêmicos, livros, normas e sites que versam sobre o assunto. Com base nessa pesquisa foi possível elaborar uma fundamentação teórica sobre temas que permeiam a cibersegurança em redes de dados de automação, assim como os seus desafios, as ações para mitigação dos riscos, além da estrutura da norma que rege a cibersegurança de sistemas de controle e automação industrial.

4. FUNDAMENTAÇÃO TEÓRICA

4.1. Infraestruturas Críticas e as ações governamentais

São consideradas infraestruturas críticas as instalações, bens e serviços que desempenham papel essencial para a sociedade e o Estado como um todo. Como exemplo de segmentos de empresas de infraestruturas críticas podemos citar: saneamento, energia, óleo e gás, transportes, saúde pública, polícia, bombeiros, forças armadas e serviços financeiros.

Essas infraestruturas são tão fundamentais que interrupções ou até mesmo a ausência da operação adequada podem acarretar num significativo impacto social, econômico, político, ambiental ou de segurança e soberania nacional (CANONGIA; GONÇALVES JR.; MANDARINO JR., 2010).

Diversos fatores podem interromper ou prejudicar a continuidade dos serviços prestados pelas infraestruturas críticas de um Estado, tais como ameaças provenientes de catástrofes da natureza, falhas de sistemas ou equipamentos e da ação humana, seja ela intencional ou não intencional (NOGUEIRA, 2012). A tabela 1 ilustra os tipos de ameaças e alguns exemplos:

Tabela 1: Tipos de ameaças e alguns exemplos (NOGUEIRA, 2012, p. 07).

TIPOS DE AMEAÇAS		EXEMPLOS
Natural		Terremoto, enchentes, deslizamento de terras, furacão, tempestade de raios, etc.
Não intencional	Falha humana	Negligência, imprudência e imperícia.
	Falha tecnológica	Erro na programação de um *software*, mau funcionamento de um equipamento eletrônico, etc.
Intencional		Terrorismo, grupo social reivindicatório, ataque criminoso, guerra declarada, etc.

Devido à relevância estratégica que possuem tais infraestruturas e os riscos e ameaças aos quais estão submetidas, os Estados estão cada vez mais preocupados e têm concentrado esforços, tomando medidas e publicando diretrizes, a fim de se protegerem das ameaças e se prepararem para eventuais incidentes que possam de alguma forma impactar no funcionamento dessas infraestruturas, identificando ações e procedimentos que permitam garantir o seu funcionamento, ainda que com alguma restrição (SANTOS; CARVALHO; CAVALCANTE, 2017).

Neste contexto, os Estados Unidos, um dos pioneiros na tarefa de proteger infraestruturas críticas, primeiramente definiram o termo, a partir da Comissão Presidencial de Proteção de Infraestrutura Crítica (PCCIP) em 1996, e em 2018 criaram uma agência federal autônoma *Cybersecurity and Infrastructure Security Agency* (CISA). A União Europeia por sua vez, publicou, em dezembro de 2006, o Programa Europeu para Proteção das Infraestruturas Críticas (PEPIC). No Brasil, diversas ações também veem sendo tomadas, como em 2018 com a publicação do decreto nº 9.573, que estabeleceu a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) e o decreto de 2020 de nº 10.569, que versa sobre a "Estratégia Nacional de Segurança de Infraestruturas Críticas" (Ensic).

4.2. Contexto histórico da Automação Industrial

Desde a pré-história que o homem procura formas de poupar esforços na realização de seu trabalho em busca de uma vida melhor. Neste contexto é que foram inventados, por exemplo, os moinhos de vento ou força animal e as rodas d'água. Estes, dentre tantos outros, são exemplos de automação num período onde ainda não haviam industrias, motivo pelo qual não podemos classificar tais técnicas como automação industrial.

Historicamente a automação industrial teve seu início durante o século XVIII, junto à 1ª Revolução Industrial. Neste momento foram criados os primeiros dispositivos semiautomáticos, como por exemplo a máquina à vapor e os teares, que elevaram significativamente a produção de artigos manufaturados. No século seguinte, com a 2ª Revolução Industrial, surge um novo conceito de automação, graças ao advento da eletricidade e a criação de dispositivos mecânicos chamados relés. Mas foi a 3ª Revolução Industrial, no século XX, que aproximou a tecnologia dos computadores à produção. O Controlador Lógico Programável (CLP), dispositivo eletrônico microprocessado, surgiu para substituir os relés mecânicos com maior confiabilidade e menor custo de materiais e mão-de-obra. Atualmente estamos vivendo a era da "Indústria 4.0", em alusão à 4ª Revolução Industrial, onde conceitos como *Internet of Things* (IoT), sistemas ciber-físicos, *Big Data*, computação em nuvem e inteligência artificial são utilizados para melhoria da eficiência e produtividade dos processos (LIMA, 2003).

Nos dias de hoje entendemos por automação qualquer sistema que faça uso de computadores a fim de substituir o trabalho humano em favor da segurança, redução de custos, qualidade dos produtos e rapidez na produção. A automação consiste na implantação de sistemas interligados e assistidos por redes de comunicação, junto à sistemas supervisórios e interfaces homem-máquina (IHM), permitindo aos operadores supervisionar os sistemas como um todo (MORAES; CASTRUCCI, 2007).

Para representar de forma gráfica e hierárquica as funções e os diferentes níveis de automação encontrados em um *Industrial Control System* (ICS), ou em português, Sistema de Controle Industrial, temos a pirâmide de automação, conforme figura 1:

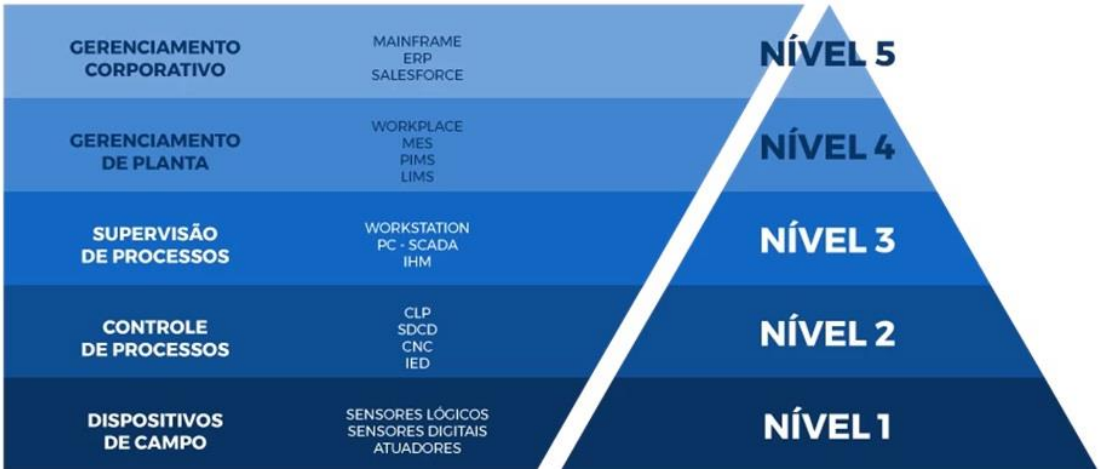

Figura 1: Pirâmide da automação (ALTUS, 2018)

Com a pirâmide de automação é possível identificar requisitos de infraestrutura e a densidade de informação que trafega entre os níveis. A ideia, dada a sua concepção, é evidenciar que a sua base comporta uma quantidade maior de dispositivos e informações, porém, as informações são melhor trabalhadas à medida que nos aproximamos do topo da pirâmide, onde o fluxo de dados diminui em quantidade e aumenta em qualidade.

Podemos descrever cada nível da pirâmide de automação, ou de forma mais técnica o Modelo *Purdue* descrito na norma ISA-95, conforme segue (MORAES; CASTRUCCI, 2007):

- **Nível 1 –** É composto por dispositivos de campo do tipo atuadores e sensores, responsáveis pela atuação no processo e aquisição de dados;
- **Nível 2 –** Contém equipamentos como os CLP's (Controlador Lógico Programável), SDCD's (Sistema Digital de Controle Distribuído) e relés e são responsáveis por controlar o processo de forma automatizada;
- **Nível 3 –** Normalmente é composto pelo sistema de supervisão e banco de dados com informações do processo, sendo o nível dedicado à supervisão e otimização dos processos;
- **Nível 4 –** Este nível é responsável pelo planejamento da produção e nele encontramos ferramentas como *Manufacturing Execution System* (MES) e *Plant Information Management System* (PIMS) para consolidação dos dados coletados no nível 3;
- **Nível 5 –** O topo da pirâmide é responsável pelo gerenciamento corporativo e administração dos recursos da empresa, como o *Enterprise Resource Planning* (ERP) e *Business Intelligence* (BI).

Conforme a necessidade de integração pode haver tráfego de dados no interior de um mesmo nível da pirâmide de automação ou então entre quaisquer um dos níveis hierárquicos. Como exemplo, dados coletados no nível 1, chão de fábrica, podem trafegar até o nível 5 para auxiliar nas tomadas de decisões, e essa transferência de dados ocorre por meio de redes de comunicação.

Quando as redes de comunicação são utilizadas para tráfego de dados de automação em qualquer nível hierárquico da pirâmide de automação, recebem o nome de redes de automação. Mais especificamente, as redes de automação podem ser divididas de três formas (CASSIOLATO, 2012):

- **Redes de Campo:** garantem a conectividade entre os mais diversos dispositivos do chão de fábrica, nível 1 da pirâmide da automação, com dispositivos como CLPs ou sistemas de supervisão SCADA (*Supervisory Control And Data Acquisition*) alocados respectivamente nos níveis 2 e 3 da pirâmide;
- **Redes de Controle:** tem como função interligar os CLPs e dispositivos de controle do nível 2 com os sistemas de supervisão do Nível 3;
- **Redes de Informação:** são as redes que representam o nível mais elevado dentro de uma arquitetura de redes de automação. Estas redes atuam nos níveis 4 e 5 da pirâmide da automação.

Em cada uma das três divisões de redes de automação apresentadas há diversos protocolos de rede disponíveis no mercado, que diferem basicamente no volume, complexidade e velocidade das informações que podem ser transmitidas e processadas. Sendo assim, é de suma importância a definição adequada das redes utilizadas para trafegar dados em todos os níveis da pirâmide da automação dentro de uma empresa e, desta forma, garantir o

gerenciamento de inúmeros processos de automação e de caráter estratégico por meio de uma ágil, precisa e segura troca de informações.

4.3. Convergência entre redes de T.I. e T.O.

A infraestrutura de TI (Tecnologia da Informação), já é bastante conhecida no mundo corporativo e muito utilizada no cotidiano. Os computadores, s*oftwares*, aplicações e diversas soluções de tecnologia, como por exemplo a *internet*, já fazem parte do dia a dia de um ambiente corporativo das empresas há muito tempo.

Por outro lado, a TO (Tecnologia Operacional), que compreende toda e qualquer forma de aplicar algum tipo de automação, controle e supervisão em ambiente industrial, sempre foi tratada de forma totalmente isolada, nas chamadas "ilhas de automação", mantendo o fluxo dos dados de automação somente no ambiente industrial da corporação. Essa distância, do ambiente de TO para com o ambiente de TI, impactou num mundo industrial com os seus próprios padrões e protocolos.

Tradicionalmente, os equipamentos, redes e *softwares* de TO eram administrados pelos departamentos de TO, enquanto a TI administrava as redes e os equipamentos corporativos no data center e nos escritórios da empresa. Eram infraestruturas totalmente distintas e separadas e, de certa forma, os colaboradores de cada uma destas áreas pouco se relacionavam. Essa estrutura funcionava muito bem, pois os equipamentos de TO não mudavam com a mesma frequência dos data centers e outros dispositivos dos ambientes de TI, que estavam em constante evolução. Atualizações de patchs, correções, implementação de cibersegurança e normas de TI eram ignoradas sem incorrer em grandes riscos para o ambiente de automação (PORTO, 2017).

Atualmente essa concepção está mudando depressa, pois estamos extraindo dados praticamente de qualquer equipamento em um ambiente industrial e utilizando esses dados em sistemas corporativos que permitem à corporação responder rapidamente às mudanças do mercado e demandas dos consumidores, ajustar a produção, realinhar seus recursos e gerenciar sua infraestrutura (PORTO, 2017). Ou seja, os dados de automação deixaram de suportar apenas o controle operacional e passaram também a ser fonte de subsídio para decisões estratégicas.

Toda essa integração entre TI e TO, motivada pela inovação digital, foi possível graças à convergência das redes de TI e TO, conforme mostra a figura 2:

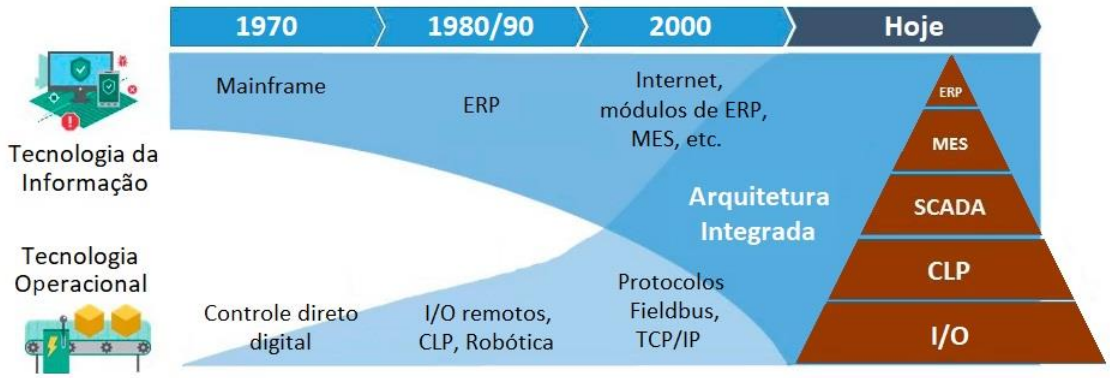

Figura 2: Convergência entre as redes de TI e TO ao longo do tempo (BRANQUINHO, 2021)

Se por um lado essa convergência possibilita novos modelos de negócio, processos mais ágeis e responsivos, traz também novos riscos consideráveis às organizações, em especial ao ambiente de TO.

Conectar uma rede de TO, que sempre esteve isolada em "ilhas de automação", à rede de TI, e, consequentemente, à intranet corporativa e *internet*, expõe a rede de TO e todos os seus dispositivos a um cenário de ameaças. Além disso, o aumento do acesso remoto às redes de TO por fornecedores terceiros aumenta ainda mais a possibilidade de ataques e cria novas vulnerabilidades. Ambientes de TO geralmente não são seguros, uma vez que foram originalmente concebidos com a suposição de que não estariam expostos a ameaças.

Compreender as necessidades e maiores vulnerabilidades das redes de TO é parte essencial do desenvolvimento de uma política de convergência entre TI e TO de sucesso. Vulnerabilidades nas redes de TO podem acarretar num impacto significativo para os negócios, comprometendo a qualidade, capacidade de produção, estabilidade financeira, podendo inclusive afetar a segurança das pessoas e o meio ambiente (BRANQUINHO, 2021). Para as organizações responsáveis por infraestruturas críticas a preocupação com estes impactos deve ser ainda maior.

4.4. Principais diferenças entre as redes de T.I. e T.O.

Apesar da convergência cada vez maior entre as redes de TI e TO, há muitas diferenças entre elas, não somente na função de cada uma delas, como também em suas prioridades.

As redes de TI são normalmente baseadas no protocolo *Ethernet* e contêm diversos *hardwares*, como, por exemplo, computadores, impressoras, servidores físicos e equipamentos de rede. Em diversos desses *hardwares* temos *softwares*, como os sistemas operacionais e os aplicativos. Todo esse conjunto, que constitui uma rede de TI, pode ser ajustado e reprogramado de muitas maneiras diferentes para atender aos requisitos de negócios e as necessidades de seus usuários, permitindo mudanças e constantes evoluções. Desta forma, as redes de TI têm como função realizar diversas operações, dentre elas, fornecer, armazenar, recuperar, transmitir, manipular e proteger dados ou informações, atendendo aos usuários dos diversos níveis hierárquicos de uma corporação.

Uma rede de TO tem a função de estabelecer a comunicação entre sensores e atuadores de processo, dispositivos controladores e sistemas de gerenciamento, supervisão e aquisição de dados. Para realizar a troca de dados e informações entre esses dispositivos e sistemas de automação utilizam-se protocolos específicos para automação conhecidos como protocolos industriais, como por exemplo, *Profinet*, *Profibus*, *Modbus*, *DeviceNet*, *EtherNet/IP*, dentre tantos outros. Muitos destes protocolos foram desenvolvidos no passado por grandes empresas fabricantes de dispositivos e equipamentos de automação. Desta forma, somente essas próprias empresas poderiam realizar manutenção nestes sistemas. Com o passar do tempo os protocolos industriais foram sendo encapsulados no TCP/IP, permitindo a comunicação com diversos fabricantes. Apesar de facilitar a troca de informação entre dispositivos, tornou as redes de TO mais vulneráveis (BRANQUINHO, 2021).

Na tabela 2 são apresentadas algumas das diferenças relevantes entre redes de TI e redes de TO:

Tabela 2: Diferenças entre redes de TI e redes de TO.

REDE DE TI	REDE DE TO
Orientada para negócios e lida principalmente com informações.	Orientada para a indústria e interage principalmente com equipamentos industriais.
Em geral não opera em tempo real.	Opera em tempo real.
Resposta tem de ser confiável.	O tempo de resposta é crítico.
Delays são aceitáveis.	*Delays* são uma séria preocupação.
Tem como objetivo a proteção dos dados e privacidade das informações.	Tem como objetivo a preservação das instalações operacionais, do meio ambiente e vida das pessoas.
Impacto dos riscos é a perda de dados e das operações dos negócios.	Impactos dos riscos são os danos aos equipamentos, perda de vidas e desastres ambientais.
Geralmente as operações são agendadas.	Operação contínua.

Falhas ocasionais são toleráveis.	Interrupções são intoleráveis.
Testes de versões beta são aceitáveis.	Testes de qualidade necessários antes da entrada em produção.
Segurança da informação e proteção de dados baseada nas normas ISSO/IEC 27000.	Diretrizes de cibersegurança baseadas na norma IEC 62443 (antiga ISA 99).

Em termos de segurança de redes, temos três conceitos importantes:

- **Confidencialidade:** previne o uso não autorizado da informação;
- **Integridade:** garante que o conteúdo da informação não foi modificado;
- **Disponibilidade:** garante que a informação esteja disponível quando requerida.

Apresentados esses três conceitos, quando pensamos em redes de TI e redes de TO há uma inversão das prioridades, conforme podemos notar na figura 3:

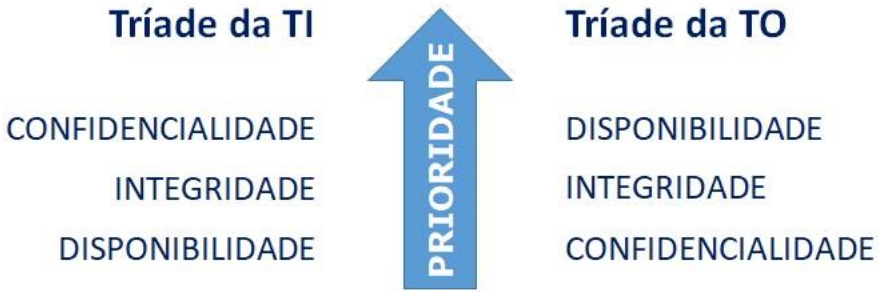

Figura 3: Tríade da TI x Tríade da TO

4.5. Breve histórico de ataques cibernéticos

Tem aumentado significativamente o número de ataques cibernéticos em ambientes de automação, especialmente em infraestruturas críticas. Isso se deve também ao fato dos ambientes de TO apresentarem baixa maturidade e consciência sobre cibersegurança. A grande maioria das redes de automação não contam com os sistemas e controles de detecção, que em geral estão presentes em ambientes de TI.

O *Stuxnet*, um vírus de computador que atacou uma usina nuclear do Irã em 2010, se transformou num marco da cibersegurança industrial. No passado os ataques cibernéticos concentravam-se em ambientes de TI, mas depois deste incidente tudo mudou. As ameaças aumentaram e os criminosos passaram a visar os ambientes de TO, incluindo as infraestruturas críticas, como um novo alvo. Os ataques cibernéticos em infraestruturas críticas podem ter os mais diferentes objetivos, como questões político-sociais, espionagem industrial e interesse financeiro (BRANQUINHO, 2021).

Como exemplos de ataques cibernéticos em empresas de infraestrutura críticas do setor de saneamento temos:

- **ETE Maroochy Shire – Austrália (2001):** Ataque ao sistema de controle da ETE Maroochy Shire, Austrália, impediu o acionamento de bombas, alarmes não estavam sendo reportados, e havia perda de comunicação entre o centro de controle e a ETE. Estes problemas causaram o alagamento do terreno de um hotel próximo, um parque, e um rio com mais de 7 milhões de litros de esgoto bruto;
- **Water Tower – EUA (2012):** Vírus enviado num documento Word por um grupo de hackers chinês, tomou conta do sistema de controle de uma torre de água, prejudicando o abastecimento de água;
- **Estação de Tratamento de Água – Flórida – EUA (2021):** Um ataque hacker em uma ETA responsável pelo fornecimento da cidade de Oldsmar, com cerca de 15 mil habitantes, tentou alterar a dosagem hidróxido de sódio de 100 para 11.000 ppm (partes por milhão). A mudança abrupta teria disparado os alarmes antes do problema se instaurar. Nenhuma residência ou morador foi afetado. Os cibercriminosos aparentemente ganharam acesso através do *software* de gerenciamento remoto *Team Viewer*.

Ao relembrarmos de alguns incidentes passados, temos a visão da dimensão dos impactos causados por um ataque cibernético em infraestruturas críticas. Conhecê-los pode auxiliar na prevenção de novos ataques e na identificação de possíveis riscos e ameaças.

5. AMEAÇAS, VULNERABILIDADES E DESAFIOS DE CIBERSEGURANÇA

O ambiente com as redes de TI e TO integradas estabelece as condições ideais para um ataque cibernético, uma vez que as redes de TI abrem portas para muitas ameaças e as redes de TO são muito vulneráveis e imaturas em relação aos controles de cibersegurança.

Na tabela 3 temos alguns exemplos que relacionam as ameaças, as vulnerabilidades, as redes impactadas e o exemplo de risco que a respectiva ameaça pode oferecer.

Tabela 3: Vetores de ataque em uma rede industrial (BRANQUINHO, 2021, p. 85)

AMEAÇA	VULNERABILIDADE	REDE	EXEMPLO DE RISCO
Ataques de negação de serviço.	Sistemas vulneráveis	Corporativa	Ataques direcionados à empresa podem impedir sua comunicação com sistemas externos ou mesmo expor outras vulnerabilidades que permitam um ataque mais direcionado.
Ataques de negação de serviço.	Sistemas vulneráveis	Controle e campo	Sistemas vulneráveis podem ser paralisados com ataques de negação de serviço simples, direcionados a dispositivos de campo e sistemas de controle.
Erro humano	Acesso remoto inseguro	Corporativa	Usuários podem vazar credenciais de acesso remoto e viabilizar a entrada de atacantes remotos.
IoT/IIoT infectado	Protocolos inseguros	Campo	Dispositivos podem vir contaminados de fábrica e interromper processos de campo de forma não programada.
Sabotagem	Baixa segurança física	Todas	Sabotadores podem alterar ou interromper processos de negócio ao comprometer dispositivos fisicamente.
Engenharia social	*Wireless* inseguro	Todas	Um atacante pode induzir colaboradores a usar uma rede não autorizada, insegura, para roubar suas credenciais e interferir no processo produtivo.
Ransomware	Dispositivos móveis	Todas	*Ransomware* pode se instalar em máquinas móveis e se alastrar quando conectado em qualquer rede da empresa.
USB infectado	Permissões incorretas	Todas	Um dispositivo USB infectado pode contaminar máquinas sem as restrições apropriadas e contaminar computadores das redes.
Script kiddies	*Software* inseguro de terceiros	Controle	Curiosos podem usar scripts da *internet* para testar a segurança de sistemas na rede de controle e comprometer seu funcionamento correto.
Infecção na operadora MPLS ou satelital	Configurações inseguras de rede	Todas	Operadoras infectadas podem vazar infecções e criar canais para criminosos que queiram interferir ou fazer mau uso da rede de automação.

As ameaças à segurança das infraestruturas críticas, e sistemas de TO em geral, crescem e trazem muita preocupação, à medida que as redes de TO se convergem com as redes de TI. Desta forma, é imprescindível evitar tais ameaças, através da adoção das melhores práticas, baseadas em normas consolidadas, bem como adotar políticas que garantam que esse tema seja tratado com a devida prioridade.

Diante deste cenário, as redes de dados de automação têm imensos desafios em relação a sua segurança. Com isso, uma série de práticas devem ser implantadas a fim de eliminar as vulnerabilidades e afastar as ameaças (BRANQUINHO, 2021). Alguns dos desafios mais comuns à maioria dos sistemas de automação, vão além da utilização de *hardware* de tecnologia avançada e *softwares* atualizados. De acordo com Branquinho (2021), temos como principais desafios de cibersegurança nas redes de TO:

- Ter a visibilidade e controle sobre os processos e aplicações que estão sendo executadas, os protocolos industriais que estão trafegando, os usuários que estão conectados e como estão atuando;
- Proteger sistemas desatualizados e mais vulneráveis através de um modelo de segurança em camadas, dificultando os ataques;
- Conviver com protocolos industriais inseguros, intensificando a visibilidade e as medidas de controle sobre eles;
- Realizar controle comportamental baseado em intensas e contínuas análises sobre a normalidade dos processos;
- Proteger a interconexão das redes de dados, planejando e implementando de forma segura a conexão das redes de TO com as demais redes da corporação.

6. NORMA ISA/IEC 62443 E AS AÇÕES PARA MITIGAÇÃO DE RISCOS

6.1. Norma ISA/IEC 62443

A ISA/IEC 62443 é uma série internacional de normas, dividida em seções, que descreve regras e conceitos relacionados à cibersegurança industrial, com o objetivo de auxiliar operadores, fabricantes de componentes e integradores de sistemas de automação industrial.

A norma oferece um guia, com os elementos necessários para implementação do *framework Cyber Security Management System* (CSMS), incluindo regras, gerenciamento de patches e requisitos para desenvolvedores de componentes de automação. O CSMS aborda a implantação de ações de segurança em ambientes de TO através de três etapas distintas e cíclicas, conforme figura 4:

Figura 4: Modelo CSMS da norma ISA/IEC 62443 (BRANQUINHO, 2021)

A norma ISA/IEC 62443 atualmente é um padrão internacional, baseado principalmente na norma ISA 99 da *International Society of Automation* (ISA). A ISA é uma organização profissional sem fins lucrativos destinada aos mais diversos profissionais do segmento de automação, dentre eles, engenheiros, técnicos, professores e estudantes, interessados em automação industrial.

Em 2002, o Comitê de Segurança do Sistema de Controle e Automação Industrial (ISA99) da ISA, desenvolveu uma série de normas e relatórios técnicos sobre o assunto da segurança de *Industrial Automation and Control Systems* (IACS). Posteriormente, o conteúdo desta série foi submetido aos grupos de trabalho da *International Electrotechnical Commission* (IEC), vindo a se tornar a ISA/IEC 62443.

A norma ISA/IEC 62443 está estruturada e dividida em seções, conforme figura 5:

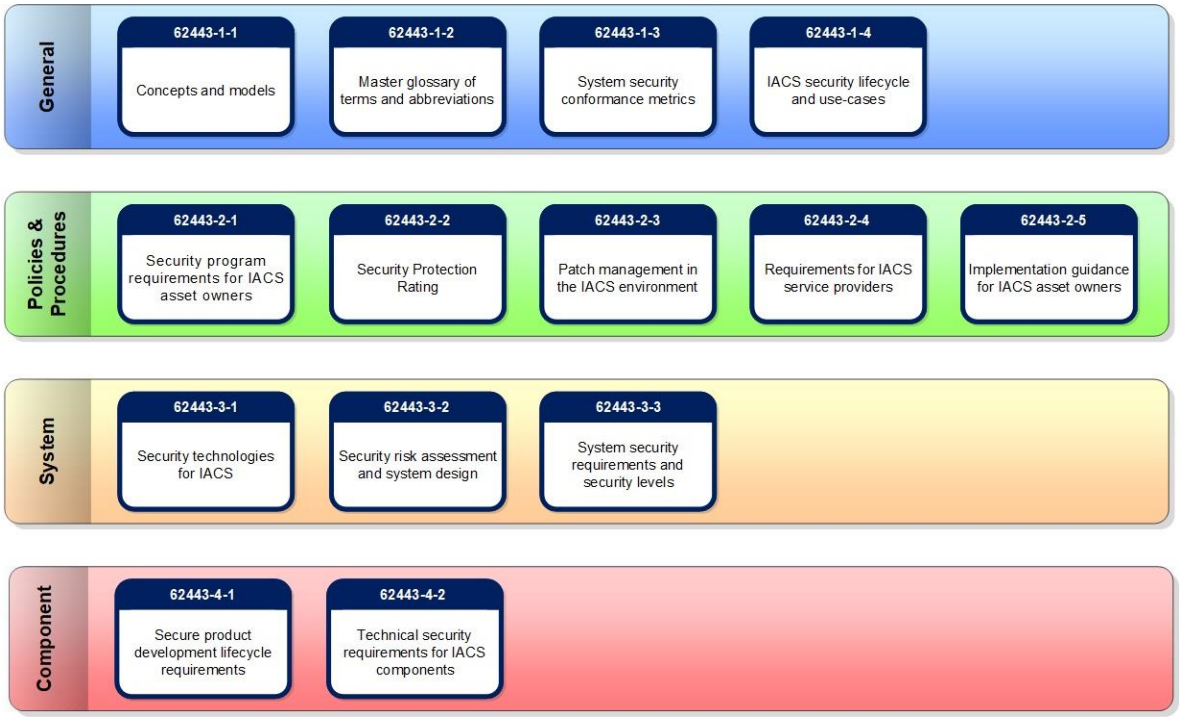

Figura 5: Norma ISA/IEC62443 (COSMAN, 2020).

Geral: Este grupo inclui documentos que abordam tópicos comuns a toda a série.

- **62443-1-1** apresenta os conceitos e modelos usados em toda a série. O público-alvo inclui qualquer pessoa que deseje se familiarizar com os conceitos fundamentais que formam a base da série.
- **62443-1-2** é um glossário mestre de termos e abreviações usados em toda a série.
- **62443-1-3** descreve uma série de métricas quantitativas derivadas dos requisitos fundamentais, requisitos do sistema e outros materiais de orientação nos padrões.
- **62443-1-4** fornece uma descrição mais detalhada do ciclo de vida subjacente para segurança IACS, bem como vários casos de uso que ilustram várias aplicações.

Políticas e Procedimentos: Os documentos deste grupo se concentram nas políticas e procedimentos associados à segurança do IACS.

- **62443-2-1** descreve o que é necessário para definir e implementar um sistema de gerenciamento de segurança cibernética IACS eficaz. O público-alvo inclui usuários finais e proprietários de ativos que são responsáveis pelo projeto e implementação de tal programa.
- **62443-2-2** fornece uma metodologia para avaliar o nível de proteção fornecido por um IACS operacional contra ameaças de segurança cibernética e como aplicar o que é exigido pelo 62443-2-1.
- **62443-2-3** fornece orientação sobre gerenciamento de patches para IACS. O público-alvo inclui qualquer pessoa responsável pelo design e implementação de uma disciplina de gerenciamento de patches.
- **62443-2-4** especifica os requisitos para fornecedores de sistemas IACS e componentes relacionados. O público principal inclui fornecedores de soluções de sistemas de controle. Este padrão foi desenvolvido pela IEC TC65 WG10.

- **62443-2-5** fornece orientação sobre o que é necessário para operar um sistema de gerenciamento de segurança cibernética IACS eficaz. O público-alvo inclui usuários finais e proprietários de ativos que são responsáveis pela operação de tal programa.

Requisitos do Sistema: Os documentos do terceiro grupo tratam dos requisitos no nível do sistema.

- **62443-3-1** descreve a aplicação de várias tecnologias de segurança a um ambiente IACS. O público-alvo inclui qualquer pessoa que deseje aprender mais sobre a aplicabilidade de tecnologias específicas em um ambiente de sistemas de controle.
- **62443-3-2** aborda a avaliação de risco de segurança e o design do sistema para IACS. Este padrão é direcionado principalmente aos proprietários de ativos ou usuários finais.
- **62443-3-3** fornece as bases para avaliar os níveis de segurança fornecidos por um sistema de automação. O público principal inclui fornecedores de sistemas de controle, integradores de sistemas e proprietários de ativos.

Requisitos de componentes: O quarto e último grupo inclui documentos que fornecem informações sobre os requisitos mais específicos e detalhados associados ao desenvolvimento de produtos IACS.

- **62443-4-1** descreve os requisitos derivados que são aplicáveis ao desenvolvimento de produtos. O público principal inclui fornecedores de produtos de sistemas de controle e de componentes incluídos em soluções de sistemas de controle.
- **62443-4-2** contém conjuntos de requisitos derivados que fornecem um mapeamento detalhado dos requisitos do sistema para subsistemas e componentes do sistema em consideração. O público principal inclui fornecedores de componentes embarcados em soluções de sistemas de controle.

É importante lembrar que a série de normas ISA/IEC 62443 pretende servir de referência, mas devem ser complementadas por diretrizes e materiais de apoio mais diretos e focados, específicos para cada corporação.

Desta forma, a ISA/IEC 62443 complementa a norma ISO/IEC 27001, que, por sua vez, reúne essencialmente os regramentos para a segurança de TI. Juntas, as normas ISA/IEC 62443 e ISO/IEC 27001 proporcionam uma abordagem abrangente para mitigação de riscos e proteção contra ameaças cibernéticas em empresas de automação, e inclusive, de infraestruturas críticas.

6.2. Análise de riscos: Análise estática e análise dinâmica

A cibersegurança em automação tem a função de analisar os riscos e vulnerabilidades existentes nos sistemas de TO e determinar as ações que devem ser adotadas para reduzir os níveis de risco de acordo com as políticas de segurança definidas pela empresa de forma contínua e ininterrupta. Essa análise deve ser realizada através de uma análise de riscos, identificando e avaliando os sistemas existentes, suas características técnicas e funcionalidades, entendendo ameaças, impactos e vulnerabilidades.

Em geral uma análise de riscos em redes de dados de automação é dividida em duas partes, sendo uma análise estática e uma análise dinâmica (BRANQUINHO, 2021).

A análise de riscos estática é realizada junto aos administradores da planta industrial e da rede de dados de automação. Trata-se de uma análise baseada no levantamento de segurança física e lógica através de questionários. Nesta análise estática são realizadas as vistorias nos ambientes de TO, verificados os diagramas da rede e respondidos os questionários. Os questionários da análise estática devem ser elaborados com base na norma internacional de cibersegurança industrial ISA/IEC 62443.

A análise de riscos dinâmica tem como objetivo verificar as ameaças e vulnerabilidades de uma rede de dados de automação através da checagem dos pacotes de dados que trafegam por esta rede. Para realização de tal análise faz-se necessário o uso de uma ferramenta de *software* conectada aos *switches* desta rede. Sem causar nenhum impacto no tráfego de dados, a ferramenta captura os dados que estão sendo trafegados na rede de automação e identifica comportamentos maliciosos, além de ser capaz de realizar um inventário dos ativos da rede.

Segundo Branquinho (2021), todo o conteúdo das análises de riscos estática e dinâmica, deverá ser consolidado num documento denominado “Relatório de Análise de Riscos”, com no mínimo os seguintes itens:

- Informação sobre os autores e agradecimento aos participantes;
- Metodologia adotada;
- Escopo das análises de riscos estática e dinâmica;
- Detalhamento dos dados obtidos, abordando a lista dos ativos, riscos encontrados por ativo, análise dos controles de segurança existentes e avaliação de conformidade;
- Recomendações para correções ou adequações;
- Resumo executivo.

6.3. Planejamento e implantação de controles de segurança cibernética industrial

Após a realização das análises de riscos e antes da implantação dos controles de cibersegurança, deve ser realizado um planejamento de cibersegurança. Subsidiado pelo relatório de análise de riscos, o planejamento tem a função de estabelecer quais os objetivos a serem alcançados, orientar como os procedimentos de segurança devem ser implementados e estipular prazos para cada ação ou projeto. No planejamento deve estar claro o nível de maturidade de cibersegurança que se almeja alcançar e quais são os riscos, detectados nas análises de riscos, que são aceitáveis e quais devem ser mitigados ou eliminados através das ações e projetos definidos no plano.

A adoção de determinados controles de segurança cibernética é de extrema importância para ajudar a mitigar os riscos de um ciberataque e alcançar a resiliência cibernética e a segurança da rede de dados de automação. Segundo Branquinho (2021), alguns dos mais importantes controles de cibersegurança industrial são:

- **Educação e conscientização:** a educação e conscientização dos responsáveis pela gestão e operação das redes de dados de automação deve ser tratada de modo contínuo, através de treinamentos, informativos, e certificação em segurança cibernética industrial. Dentre as certificações temos a ISA/IEC 62443 como a mais relevante;
- **Governança e monitoramento:** tanto a governança como o monitoramento têm como base normas, legislações e políticas de segurança da própria corporação. Novamente temos a ISA/IEC 62443 como a principal norma capaz de orientar e apontar as boas práticas para que as indústrias garantam a continuidade de seus processos;
- **Segurança de borda:** tem como objetivo principal a proteção das fronteiras da rede de dados de automação. Essa proteção atua nas conexões entre a rede de automação e as demais redes da corporação. Deve ser adotada uma arquitetura de segurança de borda adequada para cada situação, com utilização de *firewalls* e/ou zonas desmilitarizadas (DMZ);
- **Proteção da rede industrial:** além da segurança de borda, devem ser adotadas outras camadas de segurança através de conceitos como defesa em profundidade, segmentação de rede e o modelo de zonas e conduítes. Todos esses conceitos são preconizados pela norma ISA/IEC 62443;
- **Controle de malware:** existem vários tipos de malware, como os vírus, *trojan*, *worm*, *ransoware*, dentre outros. Todos esses programas maliciosos podem atuar de diversas maneiras, conforme estratégias dos atacantes;
- **Segurança de dados:** é o controle de cibersegurança que abrange as estratégias de *backup* e proteção de senhas.

6.4. Monitoramento e melhoria contínua

A última etapa, após a implantação dos controles de segurança cibernética industrial, envolve a criação de mecanismos de monitoramento e melhoria contínua.

A manutenção da segurança cibernética dos sistemas de controle e automação industrial ao longo do tempo requer revisão criteriosa e o refinamento do *framework Cyber Security Management System* (CSMS) com base nos resultados da revisão.

Devem ser considerados, como novos subsídios para se realizar a revisão do *framework* CSMS, as auditorias de conformidade de monitoramento interno, informações externas sobre contramedidas disponíveis e as leis e regulamentos, novos ou atualizados. Como resultado da revisão temos a identificação de deficiências e a proposta de melhorias no *framework* CSMS e nas ações de cibersegurança.

De posse dos resultados da revisão deve-se realizar os refinamentos do CSMS, que podem resultar em necessidades de melhoria na implementação de contramedidas, modificação de políticas e procedimentos, revisão de não conformidades, além da realização de novos treinamentos e adequação das responsabilidades organizacionais.

7. CONCLUSÕES/RECOMENDAÇÕES

A construção deste trabalho se mostrou oportuna, cumprindo com a finalidade de abordar a questão da cibersegurança em redes de TO de forma resumida, a fim de chamar atenção para o assunto e subsidiar futuras discussões sobre o tema.

Ao longo deste artigo foram abordados conceitos importantes sobre cibersegurança em redes de TO e apresentadas as principais diferenças em relação às redes de TI, motivadas por razões históricas e necessidades dissonantes. Apesar das diferenças, a evolução tecnológica culminou num processo inevitável de convergência entre as redes de TI e TO.

A convergência entre as redes de TI e TO trouxe benefícios, como gestão mais eficaz, facilidade do acesso à informação e otimização do tempo e da mão-de-obra. Isso permite que uma organização simplifique suas operações e funcione com mais eficácia, mas por outro lado se tornou um grande problema de segurança cibernética. O ambiente com as redes de TI e TO integradas, que expõe as redes de TO às ameaças oriundas da *internet*, aumenta significativamente as vulnerabilidades e as condições para um ataque cibernético.

A partir do levantamento dos principais desafios de cibersegurança para redes de TO, mencionados ao longo do presente artigo, apresentam-se alternativas possíveis para elaboração de um plano de cibersegurança e mitigação de riscos. Para isto, a norma ISA/IEC 62443 deve ser usada como referência, por se tratar de um guia de segurança cibernética de sistemas de controle e automação industrial.

Por fim, podemos concluir que a segurança cibernética em redes de TO tem a função de analisar os riscos e vulnerabilidades existentes nos sistemas de automação, engajar e treinar pessoas, e determinar as ações que devem ser adotadas para reduzir os níveis de risco de acordo com as políticas de segurança definidas pela corporação, de forma contínua e ininterrupta.

8. REFERÊNCIAS BIBLIOGRÁFICAS

1. ALTUS, Curso de Introdução à Automação [aula 01], 2018. Disponível em: https://www.altus.com.br/post/100/curso-de-introducao-a-automacao--5baula-01-5d. Acesso em: 16/05/2022.

2. BRANQUINHO, M., BRANQUINHO, T., Segurança Cibernética Industrial, Editora Alta Books, 1ª edição, 2021.

3. CANONGIA, C.; GONÇALVES JR., A.; MANDARINO JR., R. (Orgs). Guia de Referência para a Segurança das Infraestruturas Críticas da Informação. Versão 01. Brasília: GSI – Gabinete de Segurança Institucional, 2010.

4. CASSIOLATO, C., Redes Industriais – Parte 1, Revista Saber Eletrônica. Edição 461. Páginas 24 a 32, 20, 2012.

5. COSMAN, ERIC C., Structuring the ISA/IEC 62443 Standards, 2020. Disponível em: https://gca.isa.org/blog/structuring-the-isa-iec-62443-standards, Acesso em: 17/05/2022.

6. LIMA, F. S., A automação e sua evolução, Redes para Automação Industrial DCA2401 - PPGEE. Natal, Maio 2003.

7. MORAES, C. C.; CASTRUCCI, P. L., Engenharia de automação industrial, Editora LTC, 2ª edição, 2007.

8. NOGUEIRA, F., O papel do serviço de inteligência na segurança das infraestruturas críticas, Revista Brasileira de Inteligência. Brasília: Abin, n. 7, Jul. 2012.

9. PORTO, ANTONIO, À medida que a TI converge para a TO é necessária uma mudança cultural para garantir a continuidade do negócio, Blog da Schneider Electric, 2017, Disponível em: https://blog.se.com/br/gestao-de-infra-estrutura/2017/03/14/ti-to-mudanca-cultural/ Acesso em: 18/05/2022.

10. SANTOS, D. B. M.; CARVALHO, B. E. F. C.; CAVALCANTE, S. P. P., Segurança de infraestruturas críticas no Brasil, 2017.