MARCELO TEIXEIRA DE AZEVEDO

**Cibersegurança em sistemas de automação em plantas de
tratamento de água**

**São Paulo
2010**

MARCELO TEIXEIRA DE AZEVEDO

**Cibersegurança em sistemas de automação em plantas de
tratamento de água**

Dissertação apresentada à Escola Politécnica
da Universidade de São Paulo para obtenção
do título de Mestre em Engenharia

Área de Concentração: Sistemas Eletrônicos

Orientador: Prof. Dr. Sergio Takeo Kofuji

São Paulo

2010

Este exemplar foi revisado e alterado em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, de novembro de 2010.

Assinatura do autor _____

Assinatura do orientador _____

FICHA CATALOGRÁFICA

Azevedo, Marcelo Teixeira de
Cibersegurança em sistemas de automação em plantas de
tratamento de água / M.T. de Azevedo. -- São Paulo, 2010.
155 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade
de São Paulo. Departamento de Engenharia de Sistemas Eletrô-
nicos.

1. Segurança de redes 2. Ciberespaço 3. Redes de computa-
dores 4. Simulação I. Universidade de São Paulo. Escola Politéc-
nica. Departamento de Engenharia de Sistemas Eletrônicos II. t.

*A meus pais, familiares, amigos e especialmente à
Bárbara Müller.*

AGRADECIMENTOS

Agradeço ao meu orientador, Sergio Takeo Kofuji, por toda paciência e dedicação, além de toda a equipe do Grupo de Sistemas Pervasivos e de Alto Desempenho (PAD) pela ajuda direta e indireta na conclusão desta dissertação.

Em especial agradeço à minha família e amigos, por todo apoio confiado a mim e também por entender os meus momentos de ausência.

Também deixo os meus agradecimentos para Alaíde Barbosa Martins por toda ajuda, paciência e passagem de conhecimento ao longo da elaboração desta dissertação.

Agradeço também aos amigos Marco Quirino da Veiga e Fernando Muzzi, companheiros de grupo e incentivadores nos momentos de dificuldades.

Agradeço, enfim, à AT&T e IBM, empresas que confiaram e acreditaram em mim.

Se eu vi mais longe, foi por estar de pé sobre ombros de gigantes.

Isaac Newton

RESUMO

Atualmente a segurança da informação tem sido uma preocupação constante das diversas instituições e países que utilizam recursos computacionais para comunicação e oferecimento de serviços. Métodos de proteção e contramedidas para redes tradicionais são conhecidos e comumente utilizados, tais como *firewalls* e detectores de intrusões. Para os sistemas de controle e aquisição de dados (*Supervisory Control and Data Acquisition* – SCADA) não é diferente. Nos primórdios tais sistemas eram baseados em *mainframes* e arquitetura fechada, ou seja, dependentes dos fabricantes e consequentemente isolados de outros sistemas. Nos dias atuais os sistemas SCADA estão convergindo cada vez mais para plataformas baseadas em sistemas abertos e com a sua arquitetura fortemente apoiada em conectividade; sendo assim é usual a interligação de tais sistemas com a rede corporativa e em alguns casos com a própria internet. Partindo desse problema e com o atual desenvolvimento tecnológico em que se encontra a área de segurança da informação, é proposta uma metodologia para implantação de sistemas de automação em plantas de tratamento de água com ênfase em segurança e focada em sistemas industriais, utilizando as normas de segurança em automação ISA 99. Adicionalmente é proposto um mecanismo de análise e identificação de eventos maliciosos tendo por base o entendimento do fluxograma e etapas de uma planta de tratamento de água. Nesse sentido, os objetivos do presente trabalho são, em suma, estudar as normas, métodos e metodologias de segurança em sistemas industriais com foco em tratamento de água e propor uma metodologia cujo foco seja a minimização dos riscos de segurança. Para isso é proposto a avaliação de três cenários reais de tratamento de água para que assim seja possível simular os parâmetros de criticidade identificados no fluxograma e etapas do tratamento de água. Para tanto, desenvolveu-se um cenário conectado ao PLC que permitiu simular o comportamento e os impactos, além de um detector de eventos para análise dos resultados.

Palavras-chave: SCADA. Segurança. Normas ISA. Redes industriais.

ABSTRACT

Currently, information security is a constant concern of the several institutions and countries that use computing resources for communication and service offering purposes. Protection methods and countermeasures for traditional networks such as firewalls and intrusion detectors are known and ordinarily used. The same goes for control systems and data acquisition (Supervisory Control and Data Acquisition - SCADA). In the beginning, such systems were based on mainframes and closed architecture, i.e., dependent on manufacturers and consequently isolated from other systems. Nowadays, the SCADA systems converge more and more to platforms based on open systems, with its architecture strongly relied on connectivity; thus, it is usual the interconnection of such systems with the corporate network and, in some cases, with Internet itself. From this issue, and with the current technology development in the information security area, a methodology is proposed to implement automation systems in water treatment plants with an emphasis on security, and focused on industrial systems, using automation safety rules ISA 99. The purpose of this essay is, in brief, to study safety rules, methods and methodologies for industrial systems with a focus on water treatment, and to propose a methodology directed to the minimization of safety hazards. For that purpose, it is proposed the evaluation of three water treatment real scenarios so that it is possible to simulate criticality parameters identified in the flow chart and stages of the water treatment. Therefore, a scenario connected to PLC was developed, allowing the simulation of the behavior and the impacts, in addition to an event detector for the result analysis.

Keywords: SCADA. Security. Standard ISA. Industrial network.

LISTA DE FIGURAS

Figura 1 – Países com desenvolvimento avançado de ciberataques.	20
Figura 2 – Exemplo de árvore de ameaça.	35
Figura 3 – CERT: Incidentes reportados.	36
Figura 4 – CERT: Tipos de Ataque.	37
Figura 5 – Arquitetura de um Sistema SCADA.	42
Figura 6 – Componentes SCADA – (a) PLC; (b) HMI e (c) RTU.	42
Figura 7 – Arquitetura SCADA.	44
Figura 8 – Pirâmide de automação.	46
Figura 9 – Relacionamento das normas ISA 99.	47
Figura 10 – Elementos básicos do FMEA.	50
Figura 11 – Etapas do STA.	51
Figura 12 – Passos para análise do SPA.	53
Figura 13 – Processos da estação de tratamento de água (ETA).	55
Figura 14 – Estação de Tratamento de Água (ETA).	57
Figura 15 – Componentes – (a) Captação; (b) Floculação; (c) Decantação e (d) Filtragem. ...	57
Figura 16 – Componentes SCADA – (a) Bombas e (b) Painel de PLC.	58
Figura 17 – Sensor de capacidade e bomba de acionamento.	76
Figura 18 – Controle de dosagem das substâncias.	77
Figura 19 – Sistema de controle de tratamento de água.	77
Figura 20 – Ambiente Simulado.	78
Figura 21 – Cenário 1: Capital.	79
Figura 22 – Cenário 2: Interior.	80
Figura 23 – Cenário 3: Litoral.	80
Figura 24 – Cenário sugerido pela ISA 99.	81
Figura 25 – Etapas para implantação.	82
Figura 26 – Posicionamento do detector.	94
Figura 27 – Classificação do evento.	95
Figura 28 – Conversor serial para ethernet.	95
Figura 29 – OPC Cliente.	96
Figura 30 – OPC Servidor.	97
Figura 31 – Coleta de dados.	97
Figura 32 – Manipulação de variável.	101

LISTA DE GRÁFICOS

Gráfico 1 – Itens de criticidade.....	87
Gráfico 2 – Estado da bomba de captação.....	100
Gráfico 3 – Estado da bomba de captação.....	102
Gráfico 4 – Controle de dosagem.	103

LISTA DE QUADROS

Quadro 1 – Ataques realizados ao sistema de tratamento de água americano.....	19
Quadro 2 – Recomendações da ISA 99.....	88

LISTA DE TABELAS

Tabela 1 – Dosagens médias de policloreto de alumínio (ml/m ³).....	66
Tabela 2 – Vazão de água.....	73
Tabela 3 – Parâmetros da metodologia GUT.....	86
Tabela 4 – Itens de criticidade.....	87
Tabela 5 – Índice de criticidade.....	89
Tabela 6 – Índice da planta Capital.....	90
Tabela 7 – Índice da planta Interior.....	91
Tabela 8 – Índice da planta Litoral.....	92

LISTA DE ABREVIATURAS E SIGLAS

ANSI	American National Standards Institute
ASCE	American Society of Civil Engineers
AWWA	American Water Works Association
BS	British Standard
CERT	Computer Emergency Response Team
CETESB	Companhia Ambiental do Estado de São Paulo
DDOS	Distributed Denial of Service
DFMEA	Design Failure Modes and Effects Analysis
DOS	Denial of Service
ETA	Estação de Tratamento de Água
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
GPS	Global Positioning System
HAZOP	Hazard and Operability Studies
HIDS	Host-Based Intrusion Detection
HMI	Human Machine Interface
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention System
ISA	International Society of Automation
ISO	International Organization for Standardization
NIDS	Network-Based Intrusion Detection
NTU	Nephelometric Turbidity Unit
OD	Oxigênio Dissolvido
OLE	Object Linking and Embedding
OPC	OLE for Process Control
PAC	Policloreto de Alumínio
pH	Potencial Hidrogeniônico
PFMEA	Process Failure Modes and Effects Analysis
PHA	Process Hazard Analysis

PLC	Programmable Logic Controller
RADIUS	Remote Authentication Dial in User Service
RTU	Remote Terminal Unit
SABESP	Saneamento Básico do Estado de São Paulo
SCA	Sneak Circuit Analysis
SCADA	Supervisory Control and Data Acquisition
SPA	Sneak Path Analysis
SPSA	Sneak Path Security Analysis
TACACS	Terminal Access Controller Access-Control System
TCP/IP	Transmission Control Protocol / Internet Protocol
VPN	Virtual Private Network
WEF	Water Environment Federation

SUMÁRIO

1 INTRODUÇÃO	16
1.1 JUSTIFICATIVA.....	20
1.2 OBJETIVOS	23
1.3 METODOLOGIA	24
1.5 CONTRIBUIÇÕES ESPERADAS.....	24
1.4 ORGANIZAÇÃO DO TEXTO	25
2 REVISÃO DA LITERATURA.....	28
2.1 METODOLOGIAS E MODELOS PARA DETECÇÃO DE EVENTOS EM INFRAESTRUTURA CRÍTICA.....	28
2.2 SEGURANÇA EM SISTEMAS INDUSTRIAIS.....	29
2.3 SEGURANÇA EM REDES.....	30
2.4 NORMAS DE SEGURANÇA EM REDES INDUSTRIAIS	31
2.5 ANÁLISE DE RISCOS EM SISTEMAS INDUSTRIAIS	31
3 FUNDAMENTAÇÃO TEÓRICA	33
3.1 SEGURANÇA DA INFORMAÇÃO	33
3.1.1 Ameaças	34
3.1.2 Vulnerabilidades	35
3.1.3 Incidentes	36
3.2 SEGURANÇA DE REDES	37
3.2.1 Sistema de Detecção de Intrusão	37
3.2.2 Firewall	39
3.2.3 Criptografia	40
3.2.4 Tecnologias de Autenticação e Autorização	41
3.3 SISTEMAS SCADA.....	41
3.3.1 RTU.....	43
3.3.2 PLC.....	43
3.3.3 HMI.....	43
3.4 PROTOCOLOS INDUSTRIAIS	44
3.5 ARQUITETURA DA AUTOMAÇÃO INDUSTRIAL.....	45
3.6 NORMAS DE SEGURANÇA DA INFORMAÇÃO	46
3.7 METODOLOGIAS DE ANÁLISE DE RISCOS.....	48
3.7.1 FMEA	49
3.7.2 FTA	51
3.7.3 SPA	52

4 MATERIAIS E MÉTODOS	55
4.1 ESQUEMÁTICO DE UMA ESTAÇÃO DE TRATAMENTO DE ÁGUA	56
4.2 ESTAÇÃO DE TRATAMENTO DE ÁGUA	56
4.3 FLUXOGRAMA DO PROCESSO DE TRATAMENTO DE ÁGUA	59
4.4 ETAPAS DO PROCESSO DE TRATAMENTO DE ÁGUA.....	63
4.5 PARÂMETROS DE CRITICIDADE	76
4.6 CENÁRIOS	79
4.7 METODOLOGIA	81
4.8 PASSO 1: ESTABELECIMENTO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	83
4.9 PASSO 2: DEFINIÇÃO DO ESCOPO	83
4.10 PASSO 3: ANÁLISE DE RISCO.....	83
4.11 PASSO 4: GERENCIAMENTO DAS ÁREAS DE RISCO	84
4.12 PASSO 5: SELEÇÃO DOS CONTROLES E DECLARAÇÃO DE APLICABILIDADE	84
4.13 PASSO 6: IMPLEMENTAR CONTROLES.....	84
4.14 PASSO 7: AUDITORIA DO SISTEMA	85
4.15 CARACTERIZAÇÃO.....	85
5 FERRAMENTAS E SIMULAÇÕES	93
5.1 SIMULAÇÃO 01 – DESLIGAMENTO DAS DUAS BOMBAS NA CAPTAÇÃO DA ÁGUA BRUTA	99
5.1.1 Descrição.....	99
5.1.2 Resultado e Análise.....	100
5.2 SIMULAÇÃO 02 – TRANSBORDO DE ÁGUA DO TANQUE QUE RECEBE A ÁGUA TRATADA	101
5.2.1 Descrição.....	101
5.2.2 Resultado e Análise.....	101
5.3 SIMULAÇÃO 03 – DOSAGEM EXCESSIVA DE SUBSTÂNCIAS	102
5.3.1 Descrição.....	102
5.3.2 Resultado e Análise.....	102
6 CONCLUSÕES	104
6.1 TRABALHOS FUTUROS	105
REFERÊNCIAS	106
BIBLIOGRAFIA	110
APÊNDICES	112
APÊNDICE A – PUBLICAÇÕES	112
APÊNDICE B – PORTARIA Nº 518/GM, DE 25 DE MARÇO DE 2004.....	114
APÊNDICE C – CÓDIGO FONTE DOS APLICATIVOS	136

1 INTRODUÇÃO

A área de sistemas automatizados vem ganhando maior visibilidade nos últimos anos e a sua utilização torna-se cada vez mais importante para os dias atuais. Sendo uma realidade na sociedade moderna, dentre as tecnologias clássicas presentes na sociedade, pode-se destacar o comércio eletrônico, transações financeiras pela internet, telecomunicações, *VPNs*, portais de relacionamento e tantos outros sistemas informatizados que fazem parte de nosso cotidiano. A quantidade de informações presente na sociedade moderna, das quais de certa forma dependemos cada vez mais, tem evoluído de maneira crescente e métodos de defesa e práticas de segurança tornam-se necessários e devem ser estudados para garantir uma melhor proteção dessas informações sensíveis, que se atacadas podem ter grande impacto na sociedade atual, países e grupos relacionados, podendo gerar prejuízos além da indisponibilidade de serviços críticos para a sociedade, tais como:

- Distribuição de energia elétrica, água e gás;
- Atividades petroquímicas;
- Centrais nucleares;
- Controle de tráfego terrestre e aéreo.

Para os países, a indisponibilidade de serviços básicos, tais como tráfego aéreo e urbano, sinalização automobilística, saneamento, fornecimento de energia, gás e outros, pode gerar prejuízos de ordem global e até mesmo o caos na sociedade. No âmbito econômico, a indisponibilidade de sistemas críticos, como aqueles prestados por instituições financeiras, bancos e órgãos governamentais podem isolar um país.

Nas empresas dos mais diversos segmentos, o uso de práticas de segurança da informação vem sendo estudado e utilizado para minimizar os riscos apresentados, porém esse universo digital está sujeito a diversos tipos de ataques, físicos ou virtuais, que comprometem as pessoas e os sistemas a eles interligados. As práticas adotadas podem resolver parte do problema da segurança, que deve contemplar todos os recursos: computacionais, infraestrutura e recursos humanos (MARCIANO, 2006).

Diante disso, torna-se evidente o relacionamento entre o aspecto humano e computacional, para assim contribuir como um todo para a segurança da informação. Portanto as práticas de segurança da informação devem considerar os aspectos tecnológicos e humanísticos, pois dessa forma o ambiente como um todo é tratado de forma segura (MARCIANO, 2006).

Este trabalho propõe que o contexto de segurança da informação seja estudado e adequado para o ambiente no qual ele será inserido, considerando o aspecto técnico, científico e humanístico, que pode variar de empresa para empresa ou até mesmo de nação para nação. O ambiente de automação industrial, no qual em seus primórdios reinavam os sistemas proprietários e tecnologias dedicadas, era composto de sistemas fechados e sem nenhuma conectividade externa (KRUTZ, 2006). Atualmente os sistemas de automação industrial, em especial o *Supervisory Control and Data Acquisition* (SCADA – Controle Supervisório e de Aquisição de Dados), convergem para sistemas abertos e, em alguns casos, conectados à rede corporativa ou até mesmo à internet. A utilização de recursos de telecomunicação e o avanço tecnológico atual possibilitaram o acesso remoto, compartilhamento, integração e conseqüentemente o processamento de dados a distância utilizando tais recursos. Da mesma forma, tal necessidade de integração com os diversos sistemas de uma empresa está implícita na relação com os demais sistemas, visando ao aumento da produtividade e eficiência na tomada de decisões. Porém tal modelo de integração e compartilhamento pode trazer sérios problemas relacionados à segurança, pois os sistemas de controle, como dito anteriormente, eram totalmente fechados e separados do restante dos sistemas de uma empresa; assim, inseridos nesse novo contexto, fica claro que uma nova abordagem deve ser estudada.

A cada dia uma nova ameaça é registrada e ataques são realizados. Alguns ataques recentes, como no caso da Geórgia e da Rússia em relação à Ossétia do Sul, a qual é considerada uma importante rota de transporte de petróleo e gás natural na fronteira russa. A Ossétia do Sul tornou-se independente da Geórgia em 1992, após a queda da União Soviética. Sendo que Moscou apoia a Ossétia do Sul em relação à separação, mas a Geórgia não reconhece a independência (FOLHA ONLINE, 2008). Devido a esse conflito, a embaixada da Geórgia, no Reino Unido, acusou as forças na Rússia de lançar um ciberataque coordenado contra *web sites* da Geórgia, para coincidir com as operações militares na região separatista da Ossétia do Sul. Segundo o porta-voz da embaixada da Geórgia o *site* do Ministério de Defesa, escritório

presidencial e o Ministério de Negócios estrangeiros estavam indisponíveis. No entanto, o porta-voz reconheceu que, até agora, a Geórgia não pôde confirmar que a Rússia tenha sido responsável, as causas ainda estavam sob investigação (SPINER, 2008).

Outro ataque não tão recente, mas envolvendo a Estônia e novamente a Rússia, é considerado como o primeiro ataque cibernético, aconteceu em 2007 e foi motivado pela retirada de uma estátua que homenageava os soldados soviéticos mortos na Segunda Guerra Mundial, chamada de “Monumento aos Libertadores de Tallinn”, que foi transportada para um cemitério militar, fora da cidade. Devido a essa atitude, o governo da Estônia acusou a Rússia de retaliação contra o governo estoniano. Acusando os russos de indisponibilizar e invadir os *sites* da Presidência da República, do Parlamento, dos partidos políticos e dos bancos. Além de infectar com vírus e sobrecarregar os computadores governamentais. O governo russo não assume autoria do ataque e a Estônia não consegue de forma conclusiva provar que os ataques realmente são provenientes do governo russo, ou não, tendo em vista que os endereços podem ter sido trocados ou falsificados (TEIXEIRA, 2007).

Outro episódio sob investigação foi o ataque sofrido pelos Estados Unidos e Coreia do Sul, o qual pode ter sido realizado pela Coreia do Norte e grupos próximos a este país. O impacto do ataque foi a tentativa de indisponibilidade de *sites* do governo, como os da Casa Branca, dos departamentos de Defesa, de Estado, de Segurança Interna e do Tesouro, da Agência de Segurança Nacional, o da Bolsa de Valores de Nova York e o do jornal “Washington Post”. Na Coreia do Sul, entre os alvos dos ciberataques estavam o *site* da Presidência, do Ministério da Defesa, do Parlamento, do maior portal de internet do país, de bancos e do jornal “Chosun Ilbo”. Porém, a maioria dos órgãos americanos conseguiu reagir aos ataques, sofrendo com indisponibilidades momentâneas. No caso da Coreia do Sul, alguns órgãos ficaram dias inacessíveis. Da mesma forma nada de conclusivo foi diagnosticado, porém os Estados Unidos informaram a criação de um novo comando denominado *cyber command*, sob autoridade do comando estratégico americano (DNT, 2009).

Mais um evento que aconteceu nos Estados Unidos foi a invasão de uma planta de tratamento de água que ocorreu em outubro de 2006, na cidade de Harrisburg na Pensilvânia. A técnica utilizada nesse caso foi a invasão de um computador da rede e posteriormente o acesso ao sistema. A princípio, os invasores não tiveram a intenção de causar nenhum dano ao sistema de tratamento de água,

porém ficou evidente a exposição e os riscos que poderiam ter acontecido ao sistema de tratamento de água (MCMILLAN, 2006).

No Brasil existem fortes indícios que os blecautes ocorridos em 2005 no Rio de Janeiro, 2007 no Espírito Santo e em 2009 comprometendo 09 estados brasileiros, além do Paraguai, e que afetaram milhões de pessoas foram causados por invasores com o objetivo de indisponibilizar o sistema de controle, o governo brasileiro, nega tal episódio e informa que as causas foram naturais, tendo por principal causa os vendavais e temporais na região da usina (POULSEN, 2009).

Segundo Torres (2008), existe uma ordem executiva nos Estados Unidos identificada pelo número 13.010, que coloca o sistema de abastecimento de água como uma das oito estruturas críticas mais visadas e, dessa forma, estabelece necessidades de uma maior proteção. Embora a probabilidade de contaminação seja pequena, os ataques e tentativas de ataques no abastecimento de água nos Estados Unidos provaram ser um problema real, como mostrado no Quadro 1.

Quadro 1 – Ataques realizados ao sistema de tratamento de água americano.

ANO	ATACANTE	EVENTO	AGENTE
1984	Culto Religioso	Contaminação de tanques municipais que armazenavam água potável no estado de Oregon/USA	Salmonela
2001	Colaboradores do Bin Laden	Detecção de um possível evento para contaminação da distribuição de água em 28 estados americanos.	n/a
2002	Marroquinos	Desenvolvimento de ação para contaminação da tubulação de água da embaixada americana em Roma.	Cianureto
2002	Al Qaeda	Preso residente com planos e procedimento para contaminação da distribuição de água.	n/a
2003	Agentes Iraquianos	Envenenamento de alimentos e de distribuição de água.	Toxina Botulínica
n/a	Culto Religioso	Aquisição de cianureto para contaminação de parte dos reservatórios de Minneapolis	Cianureto

Fonte: Torres (2008).

Embora exista literatura muito extensa sobre mitigação, resposta e recuperação, os trabalhos estão ligadas a desastres naturais. Porém é possível

visualizar um aumento gradativo nos ataques ao sistema de distribuição de água na década atual. A *American Water Works Association (AWWA)*, a *American Society of Civil Engineers (ASCE)* e a *Water Environment Federation (WEF)* recentemente elaboraram de forma experimental um padrão comum sobre as orientações para melhorar a segurança física de instalações utilizadas para tratamento e distribuição de água potável.

Tendo esses episódios como fato, os países cada vez mais estão se preparando para conter ou até mesmo realizar ataques cibernéticos. Segundo o relatório da McAfee *Virtual Criminology Report 2009. Virtually Here: The Age of Cyber Warfare*, os países da Figura 1 são os que mais apresentam evolução na questão de cibertaquês.

Figura 1 – Países com desenvolvimento avançado de cibertaquês.

Fonte: McAfee (2009).

1.1 JUSTIFICATIVA

Atualmente os sistemas SCADA realizam funções vitais para a sociedade e estão evoluindo de maneira constante e convergindo para sistemas abertos e com a

sua arquitetura focada em conectividade. Sendo assim, torna-se muito comum a interligação dos sistemas SCADA com a intranet da empresa ou até mesmo com a internet. O sistema SCADA tem importância estratégica para uma nação tendo em vista que constitui parte dos sistemas de infraestrutura de um país, e o ataque a tais sistemas pode colocar em risco ou até mesmo isolar uma nação e prejudicar os serviços fornecidos para os seus cidadãos. Em sua grande maioria, os alvos de uma ciberguerra são os computadores, que podem ser tratados de forma individual ou em rede, e os sistemas a eles interligados. Os alvos de ataques são normalmente sistemas que controlam ou gerenciam os seguintes aspectos:

- Redes de distribuição de água potável;
- Redes de distribuição de energia elétrica;
- Redes de direção do tráfego aéreo;
- Redes de informação de emergência, tais como: polícia, bombeiro e pronto-socorro;
- Sistemas de satélite, tais como: telefonia, sinais para TV, GPS e previsão do tempo;
- Redes bancárias.

Existem muitos outros alvos que são focos de atuação de ciberterroristas, pois as possibilidades são imensas e cada vez mais a sociedade é dependente dos sistemas computacionais nos quais uma nação está inserida.

Para as possibilidades apresentadas, a sua grande maioria está automatizada e também interligada em rede, o que significa uma semelhança de arquitetura e de sistemas de automação, sendo assim explorar tais vulnerabilidades ou ganhar acesso não autorizado pode invalidar e até mesmo paralisar toda a infraestrutura de um país, bloco ou aliança de países.

Além disso, o aspecto político é uma vertente que tem crescido de forma considerável e merece ser abordado. Da mesma forma, nos últimos anos temos observado empresas privadas, públicas e instituições governamentais investindo de forma agressiva na preservação de dados confidenciais. A quantidade de ataques, porém, vem crescendo de maneira também agressiva e colocando, dessa forma, em risco a segurança das instituições dos mais diversos segmentos. Por esses fatos torna-se extremamente importante que um estudo minucioso seja realizado sobre o

assunto, além de um levantamento do histórico e da atualidade relacionada à segurança da informação, para que assim sejam propostas contramedidas para prevenção dos ataques computacionais, em especial sistemas de automação, tendo em vista que estes são responsáveis pela infraestrutura de um país.

Durante a pesquisa, verificou-se a existência de uma vasta coleção de referências (artigos, normas, livros, dissertações e teses) tratando do tema de Segurança da Informação e Segurança de Automação. Apesar dessa variedade, não se encontra facilmente uma metodologia básica ou mesmo um conjunto de diretrizes consistentes e coerentes, que auxiliem o planejamento e a implantação de um Sistema de Segurança da Informação em Redes Industriais. Visando suprir essa deficiência, este trabalho propõe uma metodologia teórico-conceitual para auxiliar a concepção, elaboração e implantação do projeto de segurança da informação baseada nas normas:

- **ANSI/ISA-TR99.00.01-2007:** *Security Technologies for Manufacturing and Control Systems;*
- **ANSI/ISA-TR99.00.02-2004:** *Integrating Electronic Security into the Manufacturing and Control Systems Environment;*
- **ANSI/ISA 99.00.01-2007:** *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models;*
- **ANSI/ISA 99.02.01-2009:** *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program;*
- **ANSI/ISA 99.00.03-2007 – Part 3:** *Operating an Industrial Automation and Control System Security Program;*
- **ANSI/ISA 99.00.04-2007 – Part 4:** *Technical Security Requirements for Industrial Automation and Control Systems.*

Trabalhos recentes discutem parte da segurança, sendo que alguns desses estudos são focados somente em elementos de segurança, tais como: *firewall*, IDS e outros. E ainda, o ambiente industrial por definição é um ambiente complexo, composto por diversos componentes, fazendo com que seja importante o seu estudo. Considerando todos esses fatores e a complexidade dos sistemas críticos, justifica-se a importância do estudo da segurança no ambiente industrial. A utilização de uma

metodologia na área de automação industrial que permita mitigar, gerenciar e propor alternativas é uma das principais motivações deste trabalho.

1.2 OBJETIVOS

O objetivo central da pesquisa é apresentar uma metodologia para a implantação da gestão de segurança da informação, tendo por base os diversos padrões e normas atuais que tratam do tema segurança da informação em automação. A aplicação da metodologia proposta gera uma série de produtos (*outputs*) e procedimentos, com os quais se busca garantir a segurança do ambiente computacional ligado em rede.

Sendo assim, a dissertação é composta por:

1. **Estudo de ambientes:** estudar e avaliar com base em cenários, topologias, normas e aplicações em redes industriais; e realizar um estudo detalhado sobre o ciclo do tratamento de água, com fluxogramas e etapas de todo o processo;
2. **Proposta de uma nova abordagem:** especificar uma nova abordagem baseada na análise e estudo crítico das normas, propondo uma metodologia para implementação com ênfase em segurança para as plantas de tratamento de água;
3. **Desenvolvimento:** criar um detector de eventos baseado nas características do ambiente e da forma de operação.

1.3 METODOLOGIA

A metodologia adotada nesta dissertação foi baseada nas seguintes etapas¹:

- Estudo e compreensão do problema e do domínio através do levantamento de referências relacionadas à análise, implantação e gestão de um sistema de segurança da informação.
- Análise crítica das normas de segurança em automação da família ISA 99.
- Levantamento do fluxograma e das etapas para o tratamento de água.
- Proposição de uma sequência de etapas para implantação de uma metodologia segura em um sistema de tratamento de água. A metodologia proposta baseou-se em diversos padrões e normas de referência na área de segurança da informação.
- Implementação e validação da metodologia proposta através da análise de 3 cenários.
- Criação de um detector de eventos baseado em situações consideradas como atos maliciosos.

1.5 CONTRIBUIÇÕES ESPERADAS

Ao término deste trabalho, espera-se obter um conhecimento sobre o funcionamento dos sistemas industriais com ênfase em segurança, para que se possa observar as principais causas que prejudicam o seu pleno funcionamento. Além de conhecer as principais limitações dessa tecnologia e principalmente a questão de segurança que tanto compromete tais sistemas. Da mesma forma, sugestões de melhorias baseadas nos estudos e normas analisadas serão propostas para um sistema de tratamento de água.

¹ Ao longo da elaboração desta dissertação, foram apresentados artigos em congressos (Apêndice A) com o intuito de discutir entre os pares a temática aqui proposta; o que trouxe grandes contribuições para a condução deste estudo.

As contribuições esperadas para esta dissertação são as seguintes:

1. **Proposta:** especificação de uma metodologia para redes industriais que tenha como a principal qualidade o aperfeiçoamento da segurança com foco em sistemas de tratamento de água funcionando como um modelo de melhores práticas a serem adotadas e contribuindo com pontos de melhorias não mencionados em tais normas. Podendo também ser adaptada para outros sistemas igualmente críticos.
2. **Análise:** a pesquisa apresentará análises críticas e comparações de normas na área de automação. Em futuros trabalhos as análises obtidas no presente trabalho podem ser utilizadas em estudos futuros ou aprimoramento de cenários e arquitetura de ambientes.
3. **Desenvolvimento:** criação de um cenário simulado e um detector de eventos baseados na definição do fluxograma e etapas estudados no processo de tratamento de água.

1.4 ORGANIZAÇÃO DO TEXTO

Para a produção desta dissertação de mestrado optou-se pela estruturação em segurança da informação num contexto global e focada em redes industriais. Complementarmente, baseou-se em estudos de normas da tecnologia da informação e de automação, para assim finalmente compor os métodos e materiais para posterior conclusão. Os capítulos são explanados de maneira mais detalhada nos tópicos a seguir.

Capítulo 2: Revisão da Literatura

Este capítulo apresenta os trabalhos relevantes relacionados com o presente trabalho, os estudos na área de interesse abaixo serão abordados:

- Metodologias e Modelos para Detecção de Eventos em infraestrutura crítica;
- Segurança em Sistemas Industriais;
- Segurança em Redes;
- Normas de Segurança em Redes Industriais;
- Análise de Riscos em Sistemas Industriais.

Capítulo 3: Fundamentação Teórica

Neste capítulo é apresentada uma introdução à temática da segurança da informação, uma análise das normas de segurança que regulamentam a área de automação e uma comparação com outras normas que tratam de segurança da informação com o foco maior em tecnologia da informação. São detalhados também os conceitos básicos de segurança da informação, sistemas SCADA, redes e protocolos industriais, como descrito a seguir:

- **Segurança da Informação e Normas:** são abordadas as principais preocupações no contexto de segurança da informação de forma geral e também em sistemas industriais. Padrões e organismos de segurança da informação serão abordados, bem como as aplicações e incidentes.
- **Sistemas SCADA:** é realizada uma introdução aos sistemas SCADA e aos componentes que fazem parte do sistema: HMI, RTU e PLC, além das suas características e responsabilidades no contexto da solução. Dessa forma, os principais fatores relacionados à segurança em sistemas industriais são abordados, além das técnicas utilizadas. Também é apresentada uma arquitetura comumente utilizada nos sistemas e métodos de um sistema industrial.

- **Protocolos Industriais:** realiza-se uma abordagem mais focada nos principais protocolos industriais que podem ser utilizados para sistemas SCADA.

Capítulo 4: Materiais e Métodos

Neste capítulo é apresentada a metodologia utilizada neste estudo, além de ser justificado o detalhamento dos passos para conclusão da metodologia. São determinados e descritos também os elementos que serão utilizados para avaliar a segurança.

Além disso, neste capítulo são detalhadas as vulnerabilidades do cenário em estudo, conforme a norma ANSI/ISA-TR 99.00.02-2004. É apresentado ainda o fluxograma de controle do processo de tratamento de água e são identificados os pontos críticos desse processo, que são estudados na tabela de análise conforme a orientação da ISA 99.

Verifica-se também neste capítulo a arquitetura de rede sugerida para esse cenário.

Capítulo 5: Ferramentas e Simulações

Neste capítulo é proposta a simulação de três eventos críticos que podem comprometer o fornecimento e a qualidade da distribuição de água potável. Ainda neste capítulo é proposto um ambiente simulado com um PLC real, um conversor de ethernet e um detector de evento.

Capítulo 6: Conclusões e Trabalhos Futuros

As devidas considerações são formuladas tendo por base o produto final da metodologia para implantação de sistemas de automação em plantas de tratamento de água com ênfase em Segurança. Os possíveis trabalhos futuros serão apresentados, bem como as linhas de pesquisa.

2 REVISÃO DA LITERATURA

Neste capítulo são analisadas e comentadas as referências bibliográficas utilizadas e que serviram de base para o desenvolvimento, estruturação e elaboração do trabalho. Todas as referências apresentam um breve resumo, objetivos e a relação com a segurança da informação. O tema proposto em sua totalidade é muito amplo e pode atuar nas mais diversas áreas do conhecimento, sendo assim as referências cobrem as diversas áreas correlacionadas na área de segurança, abordando conceitos, avaliação, aplicações, protocolos manuais e exemplos teóricos e práticos.

2.1 METODOLOGIAS E MODELOS PARA DETECÇÃO DE EVENTOS EM INFRAESTRUTURA CRÍTICA

Em “*Anomaly detection in electricity cyber infrastructures*”, Jin et al. (2010) descrevem uma metodologia para detecção de anomalias para a proteção de infraestrutura elétrica crítica, por meio da qual é aprendido o comportamento normal do sistema e, dessa forma, o perfil de tráfego torna-se conhecido. A partir desse perfil é detectado o comportamento anômalo, ou seja, que não é caracterizado dentro do perfil. Nesse sentido, os autores propõem que tal método seja utilizado para identificar ataques e falhas, podendo ser útil para informar ao operador do sistema sobre potenciais discrepâncias entre a visualização e o verdadeiro estado do sistema. O trabalho abrange duas técnicas de detecção de anomalias desenvolvidas para sistemas elétricos: indução invariante e *simulated ants*, e uma metodologia para integração. Os resultados apresentados demonstram que essa técnica tem uma contribuição significativa para a segurança da infraestrutura crítica de sistemas elétricos.

Já no trabalho “*Using model-based intrusion detection for SCADA networks*” (CHEUNG, 2006), o objetivo principal é propor um modelo para detecção de intrusos em sistemas SCADA baseado no que é esperado e aceitável em uma infraestrutura SCADA existente. Os ataques são detectados a partir da violação desse modelo, além

disso, é descrita a técnica desenvolvida e um protótipo de implementação para uma rede SCADA utilizando o protocolo Modbus.

Aplicação da metodologia para o ataque árvore em sistemas SCADA baseados no protocolo Modbus é descrita em “*The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems*” (BYRES; FRANZ; MILLER, 2004). Os autores identificam onze possíveis invasões e métodos para identificar vulnerabilidades de segurança inerentes à especificação em típicas implantações de sistemas SCADA. Estes são utilizados para sugerir as melhores práticas possíveis para operadores SCADA, além de melhorias para o protocolo Modbus.

De uma forma mais abrangente, em “*A Method for Assessment of System Security*” (ANDERSSON, 2005), é apresentado um método para se avaliar a segurança nos sistemas de informação. A base para este estudo é que a segurança é modelada tendo por parâmetro um conjunto de recursos de segurança e as suas conexões entre os componentes, e essas relações são capturadas por funções especiais que avaliam a segurança em seu contexto mais amplo. Uma ferramenta foi proposta para realizar a implementação desse método e também para demonstração dos quesitos de segurança estudado.

2.2 SEGURANÇA EM SISTEMAS INDUSTRIAIS

A melhoria de precisão e segurança dos sistemas SCADA é descrita em “*Safeguarding SCADA Systems with Anomaly Detection*” (BIGHAM; GAMEZ; LU, 2003) como podendo ser melhorada através da detecção para identificar anomalias causadas por parâmetros errados, ataques e falhas. Os desempenhos de indução invariante e *n-gram anomaly-detectors* (modelo probabilístico) são comparados nesse artigo e também é delineado um plano para integrar a saída de várias técnicas de detecção de anomalia utilizando redes *Bayesianas*. Embora os métodos indicados no artigo sejam ilustrados usando os dados de uma rede elétrica, essa pesquisa pode ter um caráter mais geral na tentativa de melhorar a segurança e a capacidade de sistemas SCADA utilizando detecção de anomalias.

Na tese de doutorado “Detecção de ataques em infraestruturas críticas de sistemas elétricos de potência usando técnicas inteligentes” (COUTINHO, 2007), o objetivo é melhorar a segurança dos sistemas SCADA. É utilizada a técnica de detecção de anomalia para identificar valores corrompidos devido a ataques ou faltas provocadas de forma maliciosa. O objetivo da tese é apresentar uma técnica alternativa para implementar detecção de anomalia para monitorar sistemas elétricos de potência.

2.3 SEGURANÇA EM REDES

Partindo do ponto de vista que os problemas recorrentes do IDS em diferenciar ataques de acessos legítimos baseados em assinaturas e não conseguir diferenciar variações desses ataques, nem tão pouco novos ataques, o estudo “*POLVO-IIDS: Um Sistema de Detecção de Intrusão Inteligente Baseado em Anomalias*” (MAFRA et al., 2008) apresenta um modelo de sistema de detecção de intrusão que classifica mensagens por análise comportamental como normal ou anômala. Para a detecção de anomalias são utilizadas duas técnicas de inteligência artificial chamadas *support vector machine* (SVM) e redes neurais de Kohonen (KNN). O uso dessas técnicas em conjunto visa melhorar a taxa de acerto do IDS desenvolvido, identificando ataques conhecidos ou novos em tempo real. Embora o artigo não trate de sistemas industriais, o método utilizado é abrangente e pode ser implementado em sistemas SCADA.

O trabalho “Segurança da Informação: uma abordagem social” (MARCIANO, 2006) realiza estudos e análises dos requisitos necessários para o tratamento da segurança da informação, utilizando-se formulações de políticas de segurança da informação. O autor baseia-se em uma estratégia de análise fenomenológica com o objetivo principal de ter uma abordagem social, de caráter humanista e com objetivos centralizados no ponto de vista dos usuários, indo ao encontro dos modelos utilizados na atualidade. Foi realizado um amplo estudo e o produto final foi um modelo para formulação de políticas de segurança da informação baseado nos domínios das ciências sociais e com uma forte ênfase nos sistemas de informação.

2.4 NORMAS DE SEGURANÇA EM REDES INDUSTRIAIS

A partir das normas ANSI/ISA 95, Amaral Filho (2005), em sua dissertação de mestrado “Requisitos para sistemas de controle de sistemas produtivos integrados a gestão”, desenvolve procedimentos para definição do escopo funcional, requisitos e modelagem para um projeto de sistemas de controle integrado à organização. O sistema atua em conformidade com os padrões técnicos e de forma estruturada com a ISA 95. O autor estabelece procedimentos para o início do projeto e definição do escopo funcional do sistema e, por fim, completa com a modelagem do sistema através do E-MFG, modelagem que suporta os padrões existentes de programação em automação.

2.5 ANÁLISE DE RISCOS EM SISTEMAS INDUSTRIAIS

Em “*Analyzing Risk and Uncertainty for Improving Water Distribution System Security from Malevolent Water Supply Contamination Events*”, Torres (2008) propõe um sistema de classificação de risco para identificação de componentes vulneráveis no sistema de distribuição de água, com forte ênfase na possibilidade de um evento intencional, como a contaminação da água. São realizadas simulações tendo por variáveis o nível inicial do tanque, os períodos do dia, a duração do evento e a quantidade de contaminantes. As medidas de prevenções são sugeridas e também é mostrado o nível de exposição.

Já em “*Risk Assessment of Power Systems SCADA*”, Hamoud, Chen e Bradley (2003) informam que falhas em sistemas SCADA podem resultar em graves consequências. De acordo com os autores, a avaliação dessas consequências na fase de planejamento pode ajudar a escolher o nível adequado de confiabilidade dos sistemas SCADA. No trabalho é apresentado um método prático para quantificar o risco associado com a falha dos sistemas, o qual primeiro identifica os riscos em vários componentes e em seguida avalia cada um considerando a sobreposição de dois eventos: falha de controle SCADA e falha de funcionamento automático da rede

de sistema de energia. O risco é calculado e expresso de forma monetária para assim realizar a classificação dos grupos de estações e consequentemente identificar a importância da estação e estabelecer os requisitos de confiabilidade para o sistema SCADA com o menor custo.

3 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo apresentam-se conceitos sobre segurança de informação aplicada a redes de computadores, com o intuito de contextualizar o trabalho realizado, caracterizar e justificar o estudo. Adicionalmente é explorado o tema de redes e protocolos industriais.

3.1 SEGURANÇA DA INFORMAÇÃO

A segurança da informação refere-se à proteção existente sobre as informações pertencentes a uma empresa ou pessoa. O assunto relativo à segurança da informação é muito abrangente e inclui inúmeras áreas do conhecimento e igualmente diversos tipos de problemas. A maior parte dos problemas de segurança é causada intencionalmente por pessoas maliciosas que tentam obter algum benefício, chamar a atenção ou prejudicar alguém. Os problemas de segurança das redes podem ser divididos nas seguintes áreas interligadas (TANENBAUM, 2003):

- **Confidencialidade:** garantir que os conteúdos de informações sigilosas sejam acessados apenas por pessoas autorizadas;
- **Autenticidade:** garantir a validade do remetente antes de expor informações sigilosas ou realizar uma transação de qualquer espécie;
- **Integridade:** assegurar que a informação transmitida pelo remetente é a mesma recebida pelo destinatário, ou seja, não sofreu nenhum tipo de alteração;
- **Irretratabilidade:** não repúdio por parte do destinatário quanto à autenticação e conteúdo de uma informação;
- **Auditoria:** verificar *logs* continuamente com o intuito de perceber possíveis invasões ou uso incorreto do sistema;
- **Disponibilidade:** garantir que um serviço esteja disponível durante um período de tempo;

- **Controle de Acesso:** assegurar que apenas usuários autorizados terão acesso a informações sigilosas.

A segurança da informação está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por elementos não autorizados, e a utilização não autorizada do computador ou de seus dispositivos periféricos. A necessidade de proteção deve ser definida em termos das possíveis ameaças, riscos e dos objetivos de uma organização, formalizados nos termos de uma política de segurança (SOARES; LEMOS; COLCHER, 1995). Os ativos da informação estão sujeitos a diversos eventos e potencialidades nocivos à sua segurança, divididos em três categorias: ameaças, vulnerabilidades e incidentes, os quais compõem e caracterizam os riscos (MARCIANO, 2006).

3.1.1 AMEAÇAS

Uma ameaça pode ser considerada como um evento ou uma atitude indesejável, podendo ser classificada como acidentais ou intencionais. Uma ameaça pode ocorrer através de diversos agentes maliciosos e consiste numa possível violação da segurança de um sistema. A materialização de uma ameaça intencional configura um ataque (SOARES; LEMOS; COLCHER, 1995).

A produção de cenários e a criação de listas de tipificação podem identificar as ameaças. A tipificação dos riscos consiste na definição de categorias e subcategorias de classificação, criando-se uma “árvore”, em que os ramos correspondem aos tipos de ameaça e as folhas às ameaças em si (SILVA; CARVALHO; TORRES, 2003), conforme ilustrado na Figura 2.

Árvore de Ameaças

Desastres ou perigos:

- de causa natural
 - ▶ provocados por água
 - cheias
 - inundações
 - ...
 - ▶ provocados por fogo
 - incêndios florestais
 - ...
 - ▶ provocados por fenómenos sísmicos
 - ▶ provocados por vento
 - tempestades
 - ▶ provocados por electricidade
 - relâmpagos
 - descargas de energia
 - ▶ provocados por agentes biológicos ou virais
 - epidemias
 - ▶ desabamentos
- com origem humana
 - ▶ acidental
 - fogo
 - inundações
 - derrames de substâncias químicas ou biológicas
 - explosões
 - queda/despiste de veículos (carros, comboios, aviões, barcos, etc.)
 - introdução incorrecta de dados nos sistemas
 - configuração incorrecta dos sistemas
 - ▶ intencional
 - quebras contratuais
 - terrorismo
 - tumultos
 - greves
 - furto
 - fraude
 - sabotagem
- ...

Figura 2 – Exemplo de árvore de ameaça.

Fonte: SILVA; CARVALHO; TORRES, (2003).

3.1.2 VULNERABILIDADES

Uma vulnerabilidade é um elemento relacionado à informação que é passível de ser explorada por alguma ameaça, representando assim um ponto potencial de falha (MARCIANO, 2006). A exploração da vulnerabilidade pode ocorrer se um determinado serviço ou sistema – pode ser um servidor ou sistema operacional, uma instalação física, aplicativo com falha – estiver em execução no ambiente.

3.1.3 INCIDENTES

Incidente é um evento que envolve uma violação da segurança podendo comprometer a confidencialidade, integridade e a disponibilidade da informação. A exploração de vulnerabilidades ocasiona os incidentes de segurança. De acordo com a Figura 3, pode-se verificar um crescimento exponencial dos incidentes ocorridos no Brasil a cada ano.

Figura 3 – CERT: Incidentes reportados.

Fonte: CERT.br (2010).

Com base nesses incidentes reportados, observa-se um aumento gradativo no início do estudo, um aumento significativo em 2003 e posteriormente outro aumento significativo em 2009. Somente nos anos de 2005 e 2007 é que foi observada uma queda confrontada com o ano anterior. Na Figura 4 podem ser observados os tipos de ataques acumulados durante o ano de 2009.

Figura 4 – CERT: Tipos de Ataque.

Fonte: CERT.br (2010).

3.2 SEGURANÇA DE REDES

A segurança é um assunto abrangente e inclui inúmeros tipos de problemas. De uma maneira simplista, a grande maioria dos problemas de segurança é causada intencionalmente por pessoas maliciosas que tentam obter algum benefício, chamar a atenção ou prejudicar alguém (TANENBAUM, 2003). Para tornar uma rede segura, é necessário utilizar mecanismos seguros para proteger a rede de todo o tipo de ameaças e ataques. No item abaixo seguem alguns mecanismos que podem ajudar na segurança de redes.

3.2.1 SISTEMA DE DETECÇÃO DE INTRUSÃO

A palavra ‘detecção’ é definida como revelar ou perceber a existência do que está escondido, enquanto que intrusão é quem ou o que se introduz em alguma parte

sem ter qualidade para tanto (FERREIRA, 2009). Sistemas de Detecção de Intrusão (do inglês, *Intrusion Detection Systems* – IDSs) são *softwares* ou *hardwares* que automatizam o processo de monitoração de eventos que ocorrem em um computador ou rede, analisando-os em busca de problemas de segurança (BACE; MELL, 2001). Como mencionado anteriormente, o ataque a redes de computadores teve um aumento significativo e a utilização de sistemas de detecção de intrusão torna-se uma ferramenta complementar para a segurança de infraestrutura como um todo.

Segundo Chebrolu, Abraham e Thomas (2004), as principais características de um IDS são:

- ser tolerante a falhas e executar continuamente com supervisão humana mínima, além de ser capaz de recuperar-se de falhas no sistema, quer seja acidental ou provocado por atividades maliciosas;
- possuir a capacidade de resistir e de detectar qualquer alteração forçada por um atacante;
- trabalhar consumindo recursos mínimos para evitar interferir com o normal funcionamento do sistema;
- ser configurado de forma precisa e de acordo com as políticas de segurança;
- ser fácil de instalar e ter portabilidade para diferentes arquiteturas e sistemas operacionais;
- detectar diferentes tipos de ataques e ter a capacidade de reconhecer atividade legítima, não confundindo com um ataque.

Os detectores de intrusão podem basear-se em:

- Assinaturas;
- Anomalias;
- Híbrida.

O IDS baseado em assinaturas possui em sua base ataques conhecidos e os dados coletados são comparados com essa base de assinatura; sendo que, caso a característica do ataque conste na base, essa tentativa é marcada como uma ameaça.

Enquanto que o IDS baseado em anomalia trabalha com desvio de comportamento. Tais desvios são sinalizados como uma possível ameaça. Já na detecção híbrida o mecanismo de análise combina as duas abordagens mencionadas anteriormente.

Os detectores de intrusão podem ser de dois tipos:

- HIDS – *Host-based intrusion detection*;
- NIDS – *Network-based intrusion detection*.

Um HIDS é instalado em determinada máquina para analisar o próprio host; isso quer dizer que não verifica outras máquinas, apenas checa a máquina onde foi instalado. Ele checa eventos como mudanças no sistema operacional, sistema de arquivos ou, ainda, tentativas de acesso a determinados arquivos.

Enquanto que o NIDS detecta ataques pela captura e análise dos pacotes que trafegam na rede. Configurado para ouvir um segmento de rede ou um *switch*, o IDS pode monitorar o tráfego da rede.

3.2.2 FIREWALL

A definição de *firewall*, segundo Cheswick, Bellovin e Rubin (2003), é uma coletânea de componentes dispostos entre duas redes, que em conjunto possuam as seguintes propriedades:

- Todo o tráfego *inbound* e *outbound* trafega pelo *firewall*;
- Somente tráfego permitido pela política de segurança pode atravessar o *firewall*;
- O *firewall* deve ser à prova de violações.

O *firewall* é um mecanismo muito usado para aumentar a segurança em redes e funciona como uma espécie de barreira de proteção. Um *firewall* pode ser visto como um monitor de referências para uma rede, sendo seu objetivo garantir a integridade dos recursos ligados a ela (SOARES; LEMOS; COLCHER, 1995).

De acordo com Cheswick, Bellovin e Rubin (2003), são três categorias em que os *firewalls* são classificados:

- Filtros de pacotes;
- *Gateways* de circuitos;
- *Gateways* de aplicação.

Os filtros de pacote utilizam endereços IP de origem e destino, e portas UDP e TCP para tomada de decisão do que é permitido ou não. Dessa forma, é elaborado uma política de segurança autorizando o tráfego de entrada e saída, e o que não se encaixa nessa permissão é negado. A abordagem baseada em filtros pode ser vulnerável no caso de uma adulteração de endereços IP.

Os *gateways* de circuitos funcionam como *proxy* TCP, atuando como intermediários de conexões. Ou seja, para transmissão de dados é necessário uma conexão do usuário com o *gateway* e este por sua vez realiza uma outra conexão através de uma nova porta TCP, formando assim um circuito para a rede interna e outro para a rede externa.

Enquanto que os *gateways* de aplicação em vez de utilizarem um mecanismo de propósito geral, como os filtros de pacotes, utilizam implementações especiais das aplicações que foram concebidas especificamente para funcionar de forma segura.

3.2.3 CRIPTOGRAFIA

A palavra ‘criptografia’ vem das palavras gregas *kriptos* e *grifos*, que significam “escrita secreta”, e surgiu devido à necessidade de se enviar informações sensíveis através de meios de comunicação não seguros (SOARES; LEMOS; COLCHER, 1995). A criptografia define uma técnica, chamada de cifragem, com o objetivo de tornar a mensagem incompreensível, de forma que somente o receptor consiga interpretar a mensagem realizando o processo de decifragem (SILVA; CARVALHO; TORRES, 2003). A utilização de chaves e algoritmos de criptografia representa um conjunto de técnicas que são utilizadas para manter a segurança da informação:

- **Simétrica ou de chave privada:** nesse algoritmo a mesma chave secreta é utilizada para cifrar e decifrar, sendo que ambos os lados devem conhecer a chave utilizada;
- **Assimétrica ou de chave pública:** são utilizadas duas chaves diferentes através de relacionamento matemático, sendo que as duas chaves são geradas a partir de uma delas, resultando uma chave pública, porém preservando o segredo da chave privada.

3.2.4 TECNOLOGIAS DE AUTENTICAÇÃO E AUTORIZAÇÃO

Autenticação é o processo de provar a própria identidade de alguém, já a autorização é quem decide quais privilégios determinado usuário terá dentro de um sistema. Nesse sentido, a autorização ocorrerá sempre após a autenticação (KUROSE; ROSS, 2003). Atualmente existem diversas formas de autenticação e autorização, entre elas podemos destacar:

- Kerberos;
- Radius;
- Tacacs e Tacacs+;
- Certificados, entre outros.

3.3 SISTEMAS SCADA

Conforme Moraes e Castrucci (2007), sistemas supervisórios são sistemas digitais de monitoração e operação da planta que gerenciam variáveis de processo. Estas são atualizadas continuamente e podem ser guardadas em bancos de dados locais ou remotos para fins de registro histórico. Um sistema SCADA provê supervisão, controle, gerenciamento e monitoramento do controle de processo dos sistemas de automação, através da coleta e análise de dados em tempo real. A prevalência dos sistemas SCADA tem crescido ao ponto que atualmente a nossa

infraestrutura depende, em grande parte, desses sistemas. Hoje, os sistemas SCADA desempenham papéis importantes em vários segmentos industriais (WILES et al., 2008).

Um sistema tradicional SCADA é composto de *Human Machine Interface* (HMI), *Programmable Logic Controller* (PLC) e *Remote Terminal Unit* (RTU). A arquitetura de tais componentes pode ser observada na Figura 5 e os componentes de arquitetura que compõem o sistema SCADA na Figura 6.

Figura 5 – Arquitetura de um Sistema SCADA.

Fonte: Próprio autor.

(a)

(b)

(c)

Figura 6 – Componentes SCADA – (a) PLC; (b) HMI e (c) RTU.

Fonte: WILES et al (2008).

3.3.1 RTU

Um RTU fornece interação inteligente de I/O para coleta e processamento, tais como leitura de interruptores, sensores e transmissores, e, em seguida, organiza os dados representativos para um formato que o sistema SCADA possa compreender. O RTU também converte valores de saída fornecidos pelo sistema SCADA de forma digital em valores que podem ser entendidos por meio de dispositivos de campo controláveis, tais como discretas (*relay*) e saídas analógicas (corrente ou tensão) (WILES et al., 2008).

3.3.2 PLC

O PLC pode ser considerado o componente principal do sistema SCADA. O controle efetivo do programa para um determinado processo ou de seus sistemas de controle é executado no PLC. O trabalho do PLC com equipamentos de entradas e saídas pode ser local, fisicamente conectado ou remotamente com as entradas e saídas fornecidas por uma RTU (WILES et al., 2008).

3.3.3 HMI

O HMI é o meio pelo qual o usuário de operação interage com o sistema SCADA. Simplificando, o HMI fornece de maneira clara e fácil, através de uma representação, o que é controlado e monitorado pelo sistema SCADA. Além disso, é possível para o operador interagir com os elementos que compõem o sistema de maneira remota.

Em uma rede SCADA, os equipamentos de campo são tipicamente conectados ao PLC, através de uma rede que utiliza protocolos independentes, tais como Fieldbus, Hart ou Modbus.

Na Figura 7 é possível visualizar a arquitetura de um sistema SCADA.

Figura 7 – Arquitetura SCADA.

Fonte: Wiles et al. (2008).

3.4 PROTOCOLOS INDUSTRIAIS

A palavra ‘protocolo’ é definida como um conjunto de regras e especificações técnicas que regulam a transmissão de dados entre computadores ou programas, permitindo a detecção e a correção de erros (FERREIRA, 2009). Os protocolos industriais surgiram para criar padrões para as redes industriais devido à necessidade de interligar os equipamentos utilizados nos sistemas de automação (ALBUQUERQUE; ALEXANDRIA, 2009). No início da utilização dos sistemas SCADA, poucos ou nenhum padrão de comunicação existia, portanto fornecedores de equipamentos criavam protocolos proprietários. Estima-se que havia entre 150 e 200 protocolos proprietários diferentes em uso. O elevado número de protocolos, juntamente com a natureza proprietária do sistema SCADA, proporcionava um grau de segurança por meio da “segurança pela obscuridade”. Como a indústria amadureceu, os sistemas SCADA começaram a adotar padrões abertos. Ou seja, o grande número de protocolos SCADA em uso foi reduzido a um pequeno número de

protocolos que estavam sendo promovidos pela indústria e organizações profissionais, que incluem, mas não limitam, os seguintes (WILES et al., 2008):

- Modbus;
- Profibus;
- Infinet;
- FieldBus;
- HART;
- UCA;
- *Distributed Network Protocol* (DNP);
- *Utility Communications Architecture* (UCA);
- *Inter-Control Center Communications Protocol* (ICCP);
- *Telecontrol Application Service Element* (TASE);
- Ethernet/IP.

3.5 ARQUITETURA DA AUTOMAÇÃO INDUSTRIAL

A arquitetura de automação industrial é representada por Moraes e Castrucci (2007) através de uma pirâmide, denominada Pirâmide de Automação. Essa pirâmide tem por principal objetivo dividir os níveis dos equipamentos envolvidos de acordo com a sua atuação na indústria e pode ser observada na Figura 8.

Sendo que:

- **Nível 1:** é o nível das máquinas;
- **Nível 2:** é o nível dos controladores digitais, dinâmicos e lógicos;
- **Nível 3:** permite o controle do processo produtivo da planta;
- **Nível 4:** responsável pela programação e planejamento da produção;
- **Nível 5:** responsável pela administração dos recursos da empresa.

Figura 8 – Pirâmide de automação.

Fonte: Moraes e Castrucci (2007).

3.6 NORMAS DE SEGURANÇA DA INFORMAÇÃO

A padronização de segurança da informação em sistemas computacionais é feita pela norma ISO/IEC 17799:2005, tendo por influência o padrão inglês BS 7799. O conjunto de normas ISO/IEC 27000 trata especificamente de padrões de segurança da informação e tornou-se um código de boas práticas para a gestão de segurança da informação, oferecendo um modelo de controle para identificação de requisitos. A identificação dos requisitos decorre da seleção de controles adequados para reduzir os riscos para valores aceitáveis (RAMOS, 2008). Já a padronização de segurança para sistemas de automação é feita pelas normas ISA 99. As normas da série ISA 99 abordam aplicações do conceito de segurança para obter os requisitos mínimos de segurança e fazem parte da série as normas abaixo.

- **ISA 99.00.01 – Part 1: Terminology, Concepts and Models.** Estabelece as terminologias, conceitos e modelos para o ambiente de automação.

- **ISA 99.00.02 – Part 2: Establishing an industrial Automation and Control System Security Program.** Descreve os elementos de gerenciamento seguro e provê orientação para as aplicações de automação industrial e sistemas de controle com segurança.
- **ISA 99.00.03 – Part 3: Operating an Industrial Automation and Control System Security Program.** Aborda como operar um ambiente de automação seguro após a concepção e implantação.
- **ISA 99.00.04 – Part 4: Technical Security Requirements for Industrial Automation and Control Systems.** Define características de automação industrial e sistemas de controle, e o que os diferencia de outros sistemas de tecnologia da informação, tendo por base o ponto de vista de segurança.

Na Figura 9 pode ser observado o relacionamento entre tais normas.

Figura 9 – Relacionamento das normas ISA 99.

Fonte: ANDERSSON, (2005).

Adicionalmente, o comitê da ISA produziu dois relatórios técnicos:

- **ANSI/ISA-TR99.00.01-2007 – *Technologies for Protecting Manufacturing and Control Systems*.** Descreve as tecnologias de segurança e o seu uso com a automação industrial e sistemas de controle.
- **ANSI/ISA-TR99.00.02-2004 – *Integrating Electronic Security into the Manufacturing and Control Systems Environment*.** Descreve como equipamentos de segurança eletrônicos podem ser integrados com a automação industrial e os sistemas de controle.

3.7 METODOLOGIAS DE ANÁLISE DE RISCOS

De acordo com Baybutt (2004), no domínio da segurança da informação, cibersegurança significava a proteção da confidencialidade, integridade e disponibilidade da informação. Para os sistemas de controle e processo, o significado de cibersegurança deve ir além disso; deve ser a proteção dos sistemas de produção, processo de controle e seus sistemas de apoio contra as ameaças dos seguintes procedimentos:

- Ataque físico ou lógico por atacantes que desejam desativar ou manipulá-los;
- Acesso por atacantes que querem obter, corromper, danificar, destruir ou proibir o acesso à informação valiosa de tais sistemas.

Existem duas abordagens para segurança cibernética, as baseadas em ativos e as baseadas em cenários. A análise baseada em ativos reflete o pensamento de segurança tradicional de proteger os itens com valor. A abordagem baseada em cenário reflete o pensamento tradicional de engenharia de processo, na proteção contra ataques específicos. É semelhante ao método de cenários proposto pela metodologia de análise de riscos denominada *Process Hazard Analysis* (PHA). Outra técnica também conhecida é a denominada estudo de perigo e operabilidade – *Hazard and Operability Studies* (HAZOP) –, usada para proteger contra acidentes e ajudar a garantir a segurança. Ambas as abordagens de segurança, baseadas em

ativos e baseadas em cenários, procuram vulnerabilidades ou fragilidades no sistema que permitem ataques bem-sucedidos (BAYBUTT, 2004).

Outras abordagens têm se mostrado úteis para estudos de sistemas de informação com forte ênfase em segurança (BAYBUTT, 2004), tais como:

- Análise dos modos de falhas e efeitos – *Failure Mode and Effects Analysis* (FMEA);
- Análise da árvore de falhas – *Fault Tree Analysis* (FTA);
- *Sneak Path Analysis* (SPA).

A seguir são descritos os três métodos:

3.7.1 FMEA

A análise dos modos de falha e efeitos é definida por Palady (2007) como uma técnica que oferece três funções distintas:

1. Ferramenta para prognóstico de problemas;
2. Procedimento para desenvolvimento e execução de projetos, processos ou serviços;
3. É o diário do projeto, processo ou serviço.

Como ferramenta mostra-se eficiente para prevenção de problemas e mostrar soluções. Aplicando como procedimento, oferece uma abordagem estruturada para o desenvolvimento de projetos e processos. Finalmente, como diário, o FMEA inicia-se na concepção do projeto, processo ou serviço, e se mantém através da vida de mercado do produto.

Atualmente existem dois tipos de FMEA:

- FMEA de projeto (*Design Failure Modes and Effects Analysis* – DFMEA);
- FMEA de processo (*Process Failure Modes and Effects Analysis* – PFMEA).

A diferença entre as duas está nos objetivos. Ambas têm objetivos diferentes e podem ser identificadas através de duas perguntas:

- Como esse projeto/processo pode deixar de fazer o que deve fazer?
- O que devemos fazer para prevenir essas falhas potenciais de projeto/processo?

Cinco elementos básicos devem ser incluídos para garantir o sucesso, e, caso um dos elementos não seja atendido, a qualidade e a confiabilidade será impactada. Na figura 10 podem ser observados os elementos básicos.

Figura 10 – Elementos básicos do FMEA.

Fonte: Palady (2007).

Os cinco elementos da Figura 10 são definidos por (PALADY, 2007):

1. Selecionar o projeto/processo;
2. Perguntar e responder às três perguntas?
 - Como pode falhar?
 - Por que falha?
 - O que acontece quando falha?

3. Implementar um esquema para identificar os modos de falha mais importantes, com o objetivo de trabalhar neles e melhorá-los;
4. Priorizar os modos de falha que serão tratados em primeiro lugar;
5. Acompanhamento se as intervenções realizadas atenderam aos objetivos, bem como realização de auditorias.

3.7.2 FTA

A definição de Limnios (2007) de FTA é uma técnica que visa melhorar a confiabilidade através de análise sistemática de possíveis falhas e consequências, adotando medidas corretivas ou preventivas. É baseado na construção de diagramas e pode utilizar de abordagens diferentes para modelar, mas a forma mais comum e popular pode ser resumida em poucas etapas. A análise envolve cinco etapas, que estão ilustradas na Figura 11.

Figura 11 – Etapas do STA.

Fonte: Adaptado de Limnios (2007).

Etapa 1: As definições de eventos indesejados é uma tarefa complexa e requer o envolvimento de pessoas qualificadas, tais como, engenheiros e analistas, para a definição do número de eventos e quais os eventos que devem ser estudados.

Etapa 2: Após a definição dos eventos, todas as causas com probabilidade de acontecer devem ser estudadas e analisadas.

Etapa 3: Definidos os eventos e analisado o sistema são descobertas as causas e efeitos de um evento indesejado e a sua probabilidade de acontecer. Dessa forma é possível construir a árvore de falhas.

Etapa 4: Depois da montagem da árvore de falhas para um evento específico, ele então é analisado e avaliado para melhorias. A gestão de riscos ocorre nessa etapa e são encontradas melhorias para o sistema e também o controle dos riscos identificados.

Etapa 5: Após a identificação das vulnerabilidades, todos os métodos possíveis são levados em consideração para diminuir a probabilidade de ocorrência.

3.7.3 SPA

Segundo Baybutt (2004), o *Sneak Path Analysis* (SPA), também conhecido como *Sneak Circuit Analysis* (SCA), tem por principal objetivo identificar caminhos inesperados ou fluxos lógicos em sistemas eletrônicos que sob certas condições podem produzir resultados indesejados ou impedir o funcionamento do sistema. Alterações do sistema podem erroneamente transparecer um problema sem importância ou com impacto local e, com isso, os operadores podem utilizar procedimentos operacionais impróprios.

Assim, pode ocorrer no *hardware*, *software* ou em ações do usuário e em alguns casos com a combinação desses três fatores. A falha no sistema é causada por situações incomuns que são disparadas independentemente dos componentes.

Portanto, o SPA é diferente de outras técnicas de análise, como a FMEA, que analisam as falhas dos componentes do sistema.

Ainda conforme Baybutt (2004), existe um paralelo para aplicação de SPA para o processo de segurança, especialmente em cibersegurança. Nesse contexto, são considerados os terroristas ou funcionários descontentes que têm por objetivo alcançar e manipular os ativos de processos: *hardware*, *software* e dados, além de informações sensíveis, como: *firewall*, senhas, criptografia, entre outros.

O ponto-chave para a análise de segurança cibernética é identificar formas ou caminhos ao longo do qual os atacantes podem penetrar os sistemas de acesso e os meios que podem utilizar para causar algum tipo de prejuízo. Alguns desses caminhos podem existir como falhas de projeto e corresponder às condições latentes de SPA convencional. Outras exigem o rompimento dos controles existentes do SPA, através da análise de barreira descrita na Figura 12.

Figura 12 – Passos para análise do SPA.

Fonte: Adaptado de Baybutt (2004).

Fase 1: Refere-se à coleta das informações necessárias para o levantamento de contramedidas para cibersegurança. Nessa fase são incluídas informações de arquitetura, configuração de rede e interfaces (interna e externa), sistemas operacionais, desenhos lógicos e físicos. O autor menciona ser necessário pensar como um terrorista, um funcionário insatisfeito ou até mesmo como um invasor externo.

Fase 2: Com o conhecimento adquirido do ambiente monta-se uma topologia representando de forma gráfica os componentes e as suas conexões.

Fase 3: Com as informações da fase 1, identifica-se os potenciais invasores que podem comprometer o ambiente. Nessa fase são considerados os possíveis invasores, sendo eles internos ou externos.

Fase 4: Da mesma forma da fase 3, os possíveis alvos e os impactos são identificados nessa fase. Podendo incluir: *hardware*, *software*, pessoas e dados.

Fase 5: Através da topologia e diagramas construídos são identificados os caminhos e combinações de alvos que podem ocasionar um problema. Em todas as análises o fluxo de caminhos possíveis deve ser considerado.

Fase 6: Nessa fase é determinado o impacto dos riscos, ou seja, a identificação dos eventos e impactos e as suas consequências. Os impactos identificados nessa fase podem ser tantos lógicos como físicos.

Fase 7: As ações são propostas com base nas análises, medidas para reduzir ou eliminar as vulnerabilidades identificadas. Assim que identificadas, as recomendações são realizadas ou são feitas sugestões de melhoria.

Fase 8: A estimativa do risco é realizada nessa fase, criando um critério de impacto e importância.

Fase 9: Nessa fase é realizado o desenvolvimento das recomendações. A necessidade de novas contramedidas ou modificações é baseada nos possíveis impactos para que as ameaças sejam reduzidas para um nível tolerável ou aceitável.

4 MATERIAIS E MÉTODOS

Para o trabalho optou-se pelo estudo de identificação de cenários de uma estação de tratamento de água. Desse modo, foi construído um sistema que refletisse todo o processo de tratamento de água. O processo de tratamento de água estudado foi o baseado no que a empresa de Saneamento Básico do Estado de São Paulo (SABESP) utiliza e disponibiliza na internet de forma pública para todos os interessados. O processo de tratamento de água da SABESP é largamente utilizado no Brasil e todo o processo que compõe o tratamento pode ser observado na Figura 13. O processo de tratamento de água estudado tem por objetivo garantir a produção de água potável, tendo por base a Portaria nº 518 do Ministério da Saúde (Apêndice B) e a Resolução SS nº 65 da Secretaria Estadual da Saúde.

Figura 13 – Processos da estação de tratamento de água (ETA).

Fonte: Próprio autor.

Porém o controle da qualidade da água é de responsabilidade da empresa que realiza o serviço de tratamento juntamente com a vigilância sanitária e CETESB. O controle da qualidade da água é realizado através de análises físico-química e microbiológicas, entre elas destaca-se:

- pH;
- sabor e odor;
- turbidez;
- cor;
- dureza;
- concentração de: cloro, flúor, alumínio, ferro, manganês, entre outros;
- determinação de OD.

4.1 ESQUEMÁTICO DE UMA ESTAÇÃO DE TRATAMENTO DE ÁGUA

O esquemático definido na Figura 13 foi ilustrado para evidenciar as etapas que compõem o processo de tratamento de água:

- Clarificação: Floculação, Decantação e Filtragem;
- Desinfecção.

Da mesma forma o fluxograma e as etapas que compõem o processo como um todo são definidos e estudados nos próximos itens.

4.2 ESTAÇÃO DE TRATAMENTO DE ÁGUA

Durante os estudos e a realização do levantamento do processo de tratamento de água, foram realizadas visitas de campo com o objetivo de entender e desenhar o

fluxograma de uma estação de tratamento de água e as etapas que compõem o processo como um todo. Na Figura 14 é possível visualizar uma Estação de Tratamento de Água (ETA) em produção, na qual todas as etapas visualizadas na seção anterior são contempladas.

Figura 14 – Estação de Tratamento de Água (ETA).

Fonte: Próprio autor.

De forma mais detalhada é possível observar na Figura 15(a) a captação da água bruta que chega até a ETA, posteriormente passa-se pelo processo de floculação, mostrado na Figura 15(b). Na Figura 15(c) pode ser observada a decantação e finalmente na Figura 15(d), a filtragem da água.

(a)

(b)

(c)

(d)

Figura 15 – Componentes – (a) Captação; (b) Floculação; (c) Decantação e (d) Filtragem.

Fonte: Próprio autor.

Já, na Figura 16(a) é mostrado as bombas de captação e na Figura 16(b), o painel de PLC que controla os sensores e atuadores.

Figura 16 – Componentes SCADA – (a) Bombas e (b) Painel de PLC.

Fonte: Próprio autor.

O produto final dessa visitação foi a elaboração de um fluxograma contendo todo o procedimento e etapas do processo de tratamento de água, que encontra-se no próximo item. No final do fluxograma é possível ver de forma descritiva todas as etapas que fazem parte do processo.

4.3 FLUXOGRAMA DO PROCESSO DE TRATAMENTO DE ÁGUA

ETAPAS

AÇÃO

12

13

14

15

16

17

18

19

ETAPAS

AÇÃO

20

21

22

23

24

25

26

27

ETAPAS

AÇÃO

28

29

30

31

32

33

34

4.4 ETAPAS DO PROCESSO DE TRATAMENTO DE ÁGUA

De forma mais detalhada é possível observar as etapas que fazem parte do fluxograma identificado no processo de tratamento de água.

➤ ETAPA 1 – CAPTAR ÁGUA

A captação de água bruta ocorre através da operação de duas Estações Elevatórias, denominadas A e B. Podendo ser realizado nos seguintes mananciais:

- Rio X;
- Ribeirão Y.

➤ ETAPA 2 – VERIFICAR TURBIDEZ, PH E OD NA CAPTAÇÃO E TURBIDEZ E PH NA CHEGADA DA ÁGUA BRUTA NA ETA

- Realizado através de turbidímetro, pHmetro e oxímetro de bancada, na Estação Elevatória.
- As análises de turbidez são efetuadas a cada hora nos seguintes pontos: mananciais (X e Y) e saída do bombeamento.
- Na chegada da água bruta na ETA, a análise de turbidez é efetuada automaticamente utilizando-se turbidímetro de processo.
- A cada hora, analisa-se o pH da água bruta na ETA através de pHmetro de bancada.

➤ ETAPA 3 – TURBIDEZ, PH E OD OK?

Conforme definição da empresa de tratamento de água, o critério de aceitação para o pH dos mananciais pode variar entre 6,0 e 7,5. Para a turbidez, o critério de aceitação é no máximo 1000 NTU. Para o OD o critério é de 5,0 a 8,0 mg/L.

Valor de turbidez acima de 1000 NTU poderá ser aceito desde que isso seja verificado nos dois mananciais e/ou a troca de manancial não seja possível.

➤ **ETAPA 4 – PROVIDENCIAR SOLUÇÃO EM FUNÇÃO DA SITUAÇÃO**

Se o pH estiver abaixo de 6,0 ou acima de 7,5, então:

- Parar bombeamento na captação;
- Decidir por troca de rio através da manobra de comportas;
- Efetuar testes;
- Acionar CETESB para averiguação.

Se a turbidez do rio estiver apresentando-se muito elevada em relação ao outro, poderá então:

- Decidir por troca de rio através da manobra de comportas;
- Efetuar testes de mistura de ambos os rios e da água bruta a tratar.

Se a turbidez de ambos os mananciais estiver elevada, acima de 500 NTU, então deve-se decidir pela utilização do Rio X com a dosagem de polímero catiônico.

Se o OD estiver abaixo de 5,0 ou acima de 8,0 mg/L, então:

- Trocar de rio através da manobra de comportas;
- Elevar a pré-cloração para no mínimo 0,3 mg/L, na água decantada, quando OD estiver abaixo de 5 mg/L;
- Acionar a CETESB em casos em que o OD analisado estiver abaixo de 2,0 mg/L, elevar a pré-cloração para no mínimo 0,3 mg/L e reduzir a vazão captada permitindo maior tempo de contato do cloro no decantador.

Valores de OD entre 5,0 mg/L e 3,0 mg/L serão aceitos, sem necessidade de manobras de comportas (trocas de mananciais), desde de que não seja identificada queda brusca (de 5,0 mg/L para 3,0 mg/L) no oxigênio do manancial. Operando com

os valores apresentados acima, deverá ser elevada a pré-cloração para no mínimo 0,3 mg/L.

➤ **ETAPA 5 – CONTROLAR PRÉ-DOSAGEM DE CAL HIDRATADA**

A pré-dosagem de cal hidratada é realizada para otimizar as condições de floculação. A não utilização dessa etapa não afeta a qualidade final da água.

➤ **ETAPA 6 – PRÉ-DOSAGEM DE CAL HIDRATADA OK?**

O critério de aceitação estabelecido para o pH da floculação está compreendido entre 4,7 e 7,0.

➤ **ETAPA 7 – CORRIGIR**

A correção é efetuada automaticamente, aumentando ou diminuindo a abertura da válvula dosadora em função da faixa de pH estabelecida, também é possível a utilização do sistema manual.

➤ **ETAPA 8 – CONTROLAR DOSAGEM DE POLICLORETO DE ALUMÍNIO (PAC)**

A dosagem é feita através de bomba dosadora provida de sinal 4-20 mA. A Tabela 2 pode ser utilizada como consulta para o ajuste inicial da dosagem de policloreto de alumínio. Porém, dependendo das características da água bruta, pode-se decidir pela utilização de outra dosagem, com base nos resultados de turbidez dos decantadores, filtros, ensaios de teste e análises de residual de alumínio dos decantadores e filtros.

Tabela 1 – Dosagens médias de policloreto de alumínio (ml/m³).

Turbidez (NTU)	10 - 30	30 - 50	50 - 100	100 - 150	150 - 200	200 - 400	Acima 400
Dosagem (ml/m ³)	9 - 23	23 - 28	28 - 35	35 - 40	40 - 47	47 - 55	Acima 55

➤ **ETAPA 9 – DOSAGEM DE POLICLORETO DE ALUMÍNIO OK?**

O critério de aceitação estabelecido conforme procedimento.

➤ **ETAPA 10 – CORRIGIR**

Se ocorrer a variação ou parada da bomba dosadora de policloreto de alumínio líquido, deve-se regular a porcentagem no gerador de sinal na sala do operador, em caso de variação na bomba dosadora.

Se a dosagem do policloreto de alumínio não for normalizada, então:

- Parar bombeamento na captação;
- Realizar a troca de bomba dosadora de policloreto de alumínio.

Se a correção da dosagem de policloreto de alumínio por bombas não for possível, deve-se utilizar sulfato de alumínio granulado. Por segurança, deve-se colocar sempre 5 mg/L a mais e, se necessário, diminuir gradualmente. É muito importante abrir a dosadora de sulfato aos poucos, pois a regulação é pouco precisa. Deve-se efetuar medição de vazão de sulfato, pH na calha Parshall e verificação da floculação a cada 15 minutos, até que as condições normais estejam restabelecidas.

Se os resultados das análises de residual de alumínio na saída dos decantadores/filtros apresentarem resultados acima do limite descritos na etapa 8, então:

- Realizar ensaio de Jar test;

- Controlar rigorosamente a pré-dosagem de cal hidratada, controlando o pH na calha Parshal e na floculação;
- Utilizar dosagem de polímero catiônico, após consulta ao Coordenador;
- Realizar análises de residual alumínio a cada 2 horas: dos decantadores, da saída dos filtros e dos reservatórios ETA I e ETA II.

Se os resultados das análises de residual alumínio na saída do ETA II apresentarem resultados acima do limite descritos na Etapa 8, então:

- Seguir as mesmas ações descritas para a saída dos filtros;
- Avaliar a situação do ETA II e, se for necessário, paralisar o abastecimento.

➤ **ETAPA 11 – CONTROLAR PRÉ-CLORAÇÃO**

É adicionado um percentual de cloro na água bruta, realizado na calha Parshall, por uma bomba que faz com que ocorra o vácuo, succionando o cloro. O residual de cloro da pré-cloração é verificado coletando a água no decantador e analisando no medidor de cloro portátil. Caso seja identificado que o limite de cor esteja acima do parâmetro máximo permitido na amostra coletada após etapa de desinfecção final, ou seja, entrada do ETA I, deverá ser elevado o percentual de cloro na pré-cloração, para que toda matéria orgânica seja oxidada.

➤ **ETAPA 12 – PRÉ-CLORAÇÃO OK?**

O critério de aceitação para a pré-cloração é de 0,1 a 0,3 mg/L, em condições normais. A amostra deve ser coletada da água decantada.

Em caso de problemas com cor, o mínimo da pré-cloração será de 0,3 mg/L, na água decantada.

➤ **ETAPA 13 – PROVIDENCIAR SOLUÇÃO PARA PRÉ-CLORAÇÃO**

Se o teor de cloro no decantador não estiver nos valores desejados, então:

- Aumentar ou diminuir o percentual de aplicação do cloro;
- Verificar bomba, tubulação e injetor de gás cloro.

➤ **ETAPA 14 – CONTROLAR FLOCULAÇÃO**

A floculação é controlada através de:

- Medição de pH, através de pHmetro de processo *on-line* inserido na 1ª câmara de floculação;
- Análise visual a cada hora através de coleta de amostras diretamente do floculador para avaliar tamanho dos flocos;
- Para auxiliar o aumento da densidade dos flocos é utilizado o polímero não iônico.

➤ **ETAPA 15 – FLOCULAÇÃO OK?**

O critério de aceitação para o pH deve ser de 4,7 a 7,0, dependendo da turbidez da água bruta, da dosagem de policloreto de alumínio e da utilização ou não de pré-dosagem de cal hidratada.

O critério de aceitação visual para a floculação é que os flocos apresentem um tamanho adequado que possibilite a decantação dos mesmos, em no máximo 10 minutos, no copo de Becker, onde a amostra foi coletada.

➤ **ETAPA 16 – CONTROLAR DECANTAÇÃO**

O controle da decantação é efetuado da seguinte forma:

- Através de análises de turbidez da água decantada, realizadas através do turbidímetro de processo (*on-line*);
- A cada duas horas, pelo operador do turno, através de coleta de amostras no local, e posterior análise de turbidez em turbidímetro de bancada.

➤ **ETAPA 17 – DECANTAÇÃO OK?**

O critério de aceitação de turbidez para o decantador é de no máximo 6,0 NTU.

➤ **ETAPA 18 – CONTROLAR FILTRAÇÃO**

A filtração é controlada da seguinte forma:

- Através de análises de turbidez da água filtrada, realizadas através de turbidímetro de processo (*on-line*);
- A cada quatro horas, ou duas vezes por turno, são coletadas, pelo operador, amostras das saídas dos quatro filtros para análise de turbidez em turbidímetro de bancada.

➤ **ETAPA 19 – FILTRAÇÃO OK?**

O critério de aceitação para a turbidez dos filtros é no máximo 0,80 NTU.

➤ **ETAPA 21 – LAVAR FILTRO**

A lavagem do filtro deve ser providenciada quando ocorrer as seguintes alternativas:

- Transpasse do filtro: quando a turbidez de saída do filtro estiver se elevando gradativamente sem que nenhuma das outras etapas anteriores do

processo também tenha se alterado. O transpasse indica que a frente de impurezas atravessou todo o meio filtrante;

- Perda de carga elevada: ocorre quando o leito filtrante encontra-se colmatado (entupido). O nível de água no interior do filtro eleva-se bastante, mesmo com o registro de abertura de filtração totalmente aberto;
- Quando o tempo de operação do filtro atingir a carreira de filtração estipulada para a lavagem periódica.

A carreira de filtração pode variar entre 24 e 56 horas, dependendo principalmente das etapas anteriores do processo e da turbidez da água bruta; sendo que a carreira de filtração é contada com o filtro em operação.

➤ **ETAPA 22 – CONTROLAR ADIÇÃO DE FLÚOR**

O controle da adição do flúor é realizado através de um sistema automatizado, monitorado por um controlador lógico programável que aciona a abertura ou fechamento da válvula de dosagem em função da análise do fluorímetro de processo, ou em modo manual.

➤ **ETAPA 24 – CONTROLAR CLORAÇÃO/DESINFECÇÃO**

É realizado através de sistema automatizado composto de analisador de cloro que controla o aumento ou diminuição da dosagem de cloro na água tratada. Realiza-se a cada 1 hora a pesagem dos cilindros para controle de consumo do produto.

➤ **ETAPA 26 – CONTROLAR PH FINAL**

O controle do pH final é realizado pela adição de cal hidratada automaticamente, através de um sistema monitorado por um CLP que aciona a abertura ou fechamento da válvula de dosagem em função do valor do pH requerido.

➤ **ETAPA 28 – CONTROLAR ADIÇÃO DE ANTICORROSIVO**

Dosagem através de bomba dosadora de solução de sal de fosfato para inibição da corrosão. A partir do controle visual, através de régua de nível, deve-se dosar 1,0 unidade de nível de solução por hora, o que é equivalente a 10 litros por hora em período seco, e 2,0 unidades de nível de solução por hora, o que é equivalente a 20 litros por hora no período úmido. A dosagem utilizada do produto é de 0,5 a 1,0 mg/L respectivamente.

➤ **ETAPA 30 – CORRIGIR**

Se os parâmetros de flúor, cloro, pH final e anticorrosivo estiverem fora dos valores estipulados nas etapas 22, 24, 26 e 28, então deve-se aumentar ou diminuir a dosagem de produtos.

➤ **ETAPA 31 – CONTROLAR TURBIDEZ E COR DA ÁGUA PRODUZIDA**

A cada hora, o operador retira uma amostra de água proveniente do reservatório para uma inspeção final da turbidez e da cor da água produzida.

➤ **ETAPA 33 – HOUVE PERDA DE FLOCULAÇÃO?**

A perda de floculação pode ocorrer devido a vários fatores, tais como:

1º - Alteração significativa no pH da água bruta (aumento ou diminuição) devido a algum despejo clandestino, não detectado junto à captação.

2º - Dosagem incorreta de policloreto de alumínio, em relação à turbidez da água bruta.

3º - Alteração da vazão da chegada da água bruta ao tratamento.

4º - Variação ou parada da bomba dosadora de policloreto de alumínio.

5º - Variação na pré-dosagem de cal hidratada.

Para cada caso devemos tomar as seguintes providências específicas que estão descritas na etapa 34.

➤ **Etapa 34 – Corrigir perda de floculação**

▪ **Caso 1º - Alteração de pH**

- a) Parar bombeamento na captação;
- b) Solicitar manobra de rio;
- c) Coletar água para teste;
- d) Abrir descarga de fundo dos floculadores;
- e) Fechar os filtros (caso perda atinja os decantadores);
- f) Abrir descarga de lavagem dos filtros;
- g) Ligar primeira bomba na captação;
- h) Acertar a floculação nos floculadores (usar tabela dosagem);
- i) Ligar segunda bomba na captação;
- j) Fechar descarga de fundo nos floculadores;
- k) Analisar turbidez nos decantadores (caminho);
- l) Fechar descargas dos filtros e iniciar filtração, quando a decantação estiver de acordo com a etapa 17;
- m) Fazer teste da mistura e do rio a ser tratado.
- n) Aumentar desinfecção final durante todo o período até que os filtros tenham voltado aos limites normais de turbidez, previstos na etapa 19.

▪ **Caso 2º - Dosagem incorreta**

- a) Diminuir vazão (parar uma bomba na captação);
- b) Abrir descarga de fundo dos floculadores;
- c) Fechar os filtros (caso perda atinja os decantadores);
- d) Abrir descarga de lavagem dos filtros;
- e) Iniciar teste com água bruta da calha Parshall;
- f) Acertar a floculação nos floculadores (usar tabela dosagem);
- g) Ligar segunda bomba na captação;
- h) Fechar descarga de fundo nos floculadores;
- i) Analisar turbidez nos decantadores (caminho);
- j) Fechar descargas dos filtros e iniciar filtração, quando a decantação estiver de acordo com a etapa 17;

- k) Aumentar desinfecção final durante todo o período até que os filtros tenham voltado aos limites normais de turbidez, previstos na etapa 19.

▪ **Caso 3º - Alteração da vazão**

- a) Abrir descarga de fundo dos flocladores;
- b) Fechar os filtros, caso a perda atinja os decantadores;
- c) Abrir descarga de lavagem dos filtros;
- d) Acertar a floclação nos flocladores, usar Tabela 2.

Esta tabela deve ser aplicada em caso do não funcionamento do medidor de vazão automático.

Tabela 2 – Vazão de água.

ALTURA DA LAMINA D'ÁGUA (CM)	VAZÃO (L/S)
30	445
31	468
32	491
33	514
34	537
35	561
36	585
37	610
38	635
39	660
40	686
41	711
42	738
43	764
44	791
45	818
46	845
47	873
48	901
49	929
50	958
51	987
52	1016
53	1046
54	1075

- e) Ligar segunda bomba na captação;
- f) Fechar descarga de fundo nos floculadores;
- g) Analisar turbidez nos decantadores;
- h) Fechar descargas dos filtros e iniciar filtração, quando a decantação estiver de acordo com a etapa 17;
- i) Aumentar desinfecção final durante todo o período até que os filtros tenham voltado aos limites normais de turbidez, previstos na etapa 19.

▪ **Caso 4º - Variação da dosagem ou parada da bomba dosadora de policloreto de alumínio**

Se a perda de floculação foi ocasionada pelo motivo citado anteriormente, então:

- a) Diminuir vazão (parar uma bomba na captação);
- b) Abrir descarga de fundo dos floculadores;
- c) Fechar os filtros (caso perda atinja os decantadores);
- d) Abrir descarga de lavagem dos filtros;
- e) Proceder conforme instruções na etapa 10 deste procedimento;
- f) Ligar segunda bomba na captação;
- g) Acertar a floculação nos floculadores (usar tabela dosagem);
- h) Fechar descarga de fundo nos floculadores;
- i) Analisar turbidez nos decantadores (caminho), no mínimo a cada 40 minutos visando avaliar a redução após a floculação estar normalizada;
- j) Fechar descargas dos filtros e iniciar filtração, quando a decantação estiver de acordo com a etapa 17;
- k) Aumentar desinfecção final durante todo o período até que os filtros tenham voltado aos limites normais de turbidez, previstos na etapa 19.

▪ **Caso 5º - Variação da pré-dosagem de cal hidratada**

Se a perda de floculação foi ocasionada pelo motivo citado anteriormente, então:

- a) Diminuir vazão (parar uma bomba na captação);
- b) Parar a pré-dosagem de cal (até a floculação normalizar).
- c) Abrir descarga de fundo dos floculadores;
- d) Fechar os filtros (caso perda atinja os decantadores);
- e) Abrir descarga de lavagem dos filtros;
- f) Ligar segunda bomba na captação;
- g) Acertar a floculação nos floculadores (usar tabela dosagem);
- h) Fechar descarga de fundo nos floculadores;
- i) Analisar turbidez nos decantadores (caminho), no mínimo a cada 40 minutos visando avaliar a redução após a floculação estar normalizada;
- j) Fechar descargas dos filtros e iniciar filtração, quando a decantação estiver de acordo com a etapa 17;
- k) Aumentar desinfecção final durante todo o período até que os filtros tenham voltado aos limites normais de turbidez, previstos na etapa 19.

Se ambos os mananciais apresentarem florescimento algal, detectado por meio da variação de alguma característica físico-química da água, tal como pH, oxigênio dissolvido, ou mesmo flotação acima do normal nos decantadores, então:

- a) Decidir pela utilização do manancial com menor concentração de algas e utilizar dosagem de carvão ativado.
- b) Acionar a CETESB para averiguação.

4.5 PARÂMETROS DE CRITICIDADE

Com base nas definições e entendimento do processo um estudo foi realizado para que fosse possível identificar os parâmetros de criticidade em uma Planta de tratamento de água. De forma que tais parâmetros identificados no processo podem ser observados nas Figuras 17 e 18.

Na Figura 17, o sensor de capacidade tem que trabalhar da forma correta, ou seja, identificando situações em que a água está além da sua capacidade ou abaixo, para que a água não transborde do tanque gerando perdas desnecessárias; da mesma forma o tanque não pode trabalhar abaixo da sua capacidade mínima. A bomba para o controle de fluxo de entrada da água é relacionada especificamente com o sensor de capacidade, que tem a função de iniciar o seu funcionamento ou parar o funcionamento da bomba.

Figura 17 – Sensor de capacidade e bomba de acionamento.

Fonte: Próprio autor.

Na Figura 18 é mostrado o controle de dosagem de substâncias químicas que devem ser conhecidas e a sua utilização respeitada, para que assim não ocorra nenhum tipo de problema com a confiabilidade e qualidade da água.

Figura 18 – Controle de dosagem das substâncias.

Fonte: Próprio autor.

Da mesma forma nas próximas etapas do processo de tratamento de água: floculação, decantação, filtração e até o final do processo como um todo são observados os sensores de capacidade, bomba para acionamento da hélice, pá, temporizador para remoção da água suja e transporte de água de um estágio para outro.

Com base no processo, fluxograma e etapas, criou-se uma simulação de todo o processo descrito por meio do desenvolvimento de um sistema, utilizando linguagem C# (Apêndice C); com objetivo principal de ser um sistema de controle, supervisão e aquisição de dados, para que fosse possível realizar a operação de uma estação de tratamento de água e acompanhar o comportamento do tráfego e o impacto dos parâmetros de criticidade. Na Figura 19 é ilustrada a tela do sistema desenvolvido.

Figura 19 – Sistema de controle de tratamento de água.

Fonte: Próprio autor.

Na Figura 20 é possível observar o ambiente simulado com o sistema de controle e aquisição de dados e os componentes da rede industrial. O PLC se comunicará diretamente com o sistema através do protocolo OPC e do conversor de ethernet. Um gerador de tráfego é posicionado estrategicamente para que possibilite a comunicação com o PLC via rede ethernet. Para que todo o tráfego de rede seja identificado, um analisador de protocolo foi utilizado para monitorar o tráfego, bem como a comunicação entre o servidor e o cliente. Da mesma forma o detector de intrusão é posicionado na rede de forma estratégica para que consiga capturar os dados e posteriormente enviá-los para análise e conclusão das informações disponibilizadas.

Para a concretização dos testes foi realizada a comunicação do PLC diretamente com o sistema através do protocolo OPC e um conversor de ethernet. Um gerador de tráfego foi posicionado estrategicamente para que gerasse comunicação com o PLC via rede ethernet. Para a coleta do tráfego de rede, um analisador de protocolo de rede foi utilizado para monitorar o ambiente e a comunicação entre o servidor e o cliente.

Figura 20 – Ambiente Simulado.

Fonte: Próprio autor.

4.6 CENÁRIOS

Para o estudo de caso foi realizado o levantamento de três cenários típicos utilizados no processo de tratamento de água, denominados:

- Cenário Capital
- Cenário Interior
- Cenário Litoral

Nesses cenários poderão surgir falhas de segurança se a política de segurança não se adequar ao ambiente, podendo ocorrer assim o comprometimento das informações globais do sistema. Tais cenários serão analisados tendo por ponto de partida as definições das normas e acentuando-se as diferenças com o emprego da implantação da segurança. Os cenários estudados estão descritos nas Figuras 21, 22 e 23.

Figura 21 – Cenário 1: Capital.

Figura 22 – Cenário 2: Interior.

Figura 23 – Cenário 3: Litoral.

Adicionalmente, na Figura 24, é possível visualizar o diagrama de uma arquitetura recomendada pela norma ISA 99, a qual estabelece um forte foco na parte

de segurança. No próximo capítulo tais cenários serão avaliados através das normas ISA 99, com o objetivo principal de se verificar a questão de segurança.

Figura 24 – Cenário sugerido pela ISA 99.

4.7 METODOLOGIA ADOTADA

Neste item objetiva-se oferecer uma metodologia para implantação de uma Planta de tratamento de água com forte ênfase em segurança da informação, partindo dos estudos e da análise de três outras metodologias:

- FMEA;
- FTA;
- SPA.

Note que essa metodologia provavelmente não conseguirá atender por completo às especificidades de uma dada organização, porém esta poderá servir

como referencial inicial para o processo de implantação em uma determinada empresa. A metodologia aqui descrita segue as recomendações da ISA 99 e demais normas já mencionadas. A implantação do sistema proposto parte do princípio da padronização e documentação dos procedimentos, das ferramentas e das técnicas utilizadas, além da criação de indicadores, registro e de todo um processo educacional de conscientização (MARTINS; SANTOS, 2005). As etapas que compõem o processo são apresentadas na Figura 25.

Figura 25 – Etapas para implantação.

Fonte: Martins e Santos (2005).

4.8 PASSO 1: ESTABELECIMENTO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Para construir a política de segurança da organização, deve-se tomar por base os padrões e normas já citados no capítulo 2. Isso porque a política de segurança é um documento que deve descrever as recomendações, as regras, as responsabilidades e as práticas de segurança em conformidade com as especificações e necessidades da empresa. Dessa forma a elaboração de uma política de segurança é uma tarefa complexa que necessita ser revisada e alterada de forma constante.

4.9 PASSO 2: DEFINIÇÃO DO ESCOPO

Para definição do escopo, deve-se envolver o levantamento dos ativos que farão parte da política de segurança, entre eles destacam-se: equipamentos industriais, sistemas, estrutura de comunicação, pessoas, serviços e infraestrutura de rede interna e externa. Esse passo produz os seguintes resultados: mapa do perímetro da rede, inventário e classificação dos ativos.

4.10 PASSO 3: ANÁLISE DE RISCO

Nesse passo realiza-se a análise de segurança para o escopo definido anteriormente, ou seja, através da identificação dos ativos de informação envolvidos e do mapeamento de todas as ameaças relacionadas a estes. Para cada ameaça deve-se determinar o nível de risco envolvido. Após a análise de risco são definidos quais são os riscos aceitáveis e os não aceitáveis.

4.11 PASSO 4: GERENCIAMENTO DAS ÁREAS DE RISCO

Esse passo é um processo contínuo, que não termina com a colocação em prática de uma medida de segurança. A monitoração constante torna-se um recurso em que é possível identificar o sucesso da aplicabilidade e também para a realização de revisões e ajustes. Nessa etapa é estimado o impacto que um determinado risco pode causar ao negócio. Sendo assim, é preciso identificar os ativos e as vulnerabilidades mais críticas, possibilitando a priorização dos esforços e os gastos com segurança. Uma vez que os riscos tenham sido identificados e a organização tenha definido quais serão tratados, as medidas de segurança devem ser de fato implementadas.

4.12 PASSO 5: SELEÇÃO DOS CONTROLES E DECLARAÇÃO DE APLICABILIDADE

Os controles devem ser selecionados e colocados em prática para assegurar que os riscos sejam reduzidos a um nível que não possam trazer problemas para a empresa. Isso deve ocorrer após a identificação dos requisitos.

4.13 PASSO 6: IMPLEMENTAR CONTROLES

Os processos de implantação de contramedidas e de diretivas de segurança ocorrem durante toda a fase de implantação da metodologia. Em seguida, deve ocorrer um processo de acompanhamento de todos os controles implementados e, para isso, é necessária a produção de indicadores específicos que possibilitem visualizar as condições de funcionamento e desempenho do ambiente analisado. A implementação dos controles selecionados pode envolver a aquisição de tecnologia de *software* e/ou *hardware* (custos adicionais), mas, em alguns casos, essa

implementação resulta apenas na criação de padrões e normas internas a serem obedecidas (MARTINS; SANTOS, 2005).

4.14 PASSO 7: AUDITORIA DO SISTEMA

As auditorias de sistema têm por principal objetivo verificar, com base em evidências claras, se as seguintes condições ocorrem satisfatoriamente (MARTINS; SANTOS, 2005):

- a. os procedimentos e instruções operacionais são adequados e eficazes;
- b. os setores da empresa vêm atuando em concordância com os documentos normativos;
- c. os subsídios fornecidos são suficientes para elaboração dos relatórios periódicos de análise crítica.

4.15 CARACTERIZAÇÃO

Neste item os cenários descritos no capítulo 3 foram submetidos para avaliar o índice de segurança com base na planilha de controle da ISA 99 e com a utilização da metodologia GUT. Por fim, foram sugeridas recomendações de melhorias.

Passo 1: Nenhum dos cenários apresentados proporcionava uma política de segurança clara e objetiva. A preocupação com o nível de segurança, ou seja, a utilização de técnicas e equipamentos de segurança ficava a cargo do responsável pela Planta de automação. Sendo assim foi necessária a estruturação de um plano de ação para implantação de uma política de segurança da informação. É importante ressaltar que a criação de uma política de segurança não deve ser tratada de maneira isolada, ela deve ser apresentada para todos os funcionários e um processo de

conscientização faz-se necessário para garantir que os princípios dessa política sejam seguidos por todos os usuários da empresa.

Passo 2: O levantamento dos ativos envolvidos é necessário para a definição do escopo. É muito importante a análise de custo benefício para a definição do escopo assumido para a implantação dos controles, uma vez que quanto maior o escopo maior a complexidade e, conseqüentemente, maior será o investimento. O levantamento dos ativos ocorreu de forma manual e o levantamento gerou os cenários descritos no capítulo 3.

Passo 3: Para realizar o levantamento de prioridades de segurança foi utilizada a metodologia GUT, que tem por objetivo avaliar cada fator, levando em consideração os critérios de gravidade, urgência e tendência. Os parâmetros e os respectivos valores a serem referidos a cada aspecto são mostrados na Tabela 3.

Tabela 3 – Parâmetros da metodologia GUT.

VALOR	GRAVIDADE	URGÊNCIA	TENDÊNCIA
1	Sem gravidade	Não tem pressa	Não vai piorar
2	Pouco grave	Pode esperar um pouco	Vai piorar em longo prazo
3	Grave	O mais cedo possível	Vai piorar em médio prazo
4	Muito grave	Com alguma urgência	Vai piorar em pouco tempo
5	Extremamente grave	Ação imediata	Vai piorar rapidamente

A gravidade diz respeito ao impacto causado à estação de tratamento de água para o fornecimento de água potável. Já a urgência está vinculada ao tempo para diminuir ou excluir o problema, e a tendência está associada ao impacto futuro no caso de nenhuma ação ser feita em relação ao problema. Dessa forma foi realizado todo o levantamento em relação aos pontos de criticidade que podem afetar a segurança em plantas de tratamento de água. Na Tabela 4, a seguir, tais itens podem ser visualizados.

Tabela 4 – Itens de criticidade.

ITEM	G	U	T	TOTAL
<i>Firewall</i>	5	5	5	125
<i>Firewall</i> com redundância	3	4	3	26
Equipamentos com autenticação	5	5	4	100
Criptografia	3	3	3	27
Criptografia forte	2	2	2	8
IDS	5	4	3	60
Equipamentos atualizados	5	5	5	125
<i>Virtual Private Network</i>	4	3	2	24
Monitoração	2	4	4	32
Controle de acesso físico	4	5	5	100
Atualizações periódicas	3	3	3	27
<i>Virtual Local Network</i>	5	3	3	45

No Gráfico 1 é possível visualizar a representação gráfica dos itens de criticidade, sendo que os itens mais críticos são: ausência de *firewall*, equipamentos desatualizados e controle de acesso físico.

Gráfico 1 – Itens de criticidade.

Fonte: Próprio autor.

Passo 4: Os controles necessários para proteger os ativos devem ser definidos após a análise de risco de forma que o processo de identificação dos riscos e implantação dos controles deve ser tratado de forma contínua. Com o levantamento realizado na etapa anterior, tornou-se possível mensurar o impacto que um determinado risco pode causar, e, assim, foi possível implantar os controles apenas para as situações mais críticas, afinal torna-se muito difícil oferecer proteção total contra todas as ameaças existentes.

Passo 5: Neste passo, os controles apresentados pela ISA 99 foram selecionados os aplicáveis à organização. Tendo por ponto de partida as normas ISA 99, foi estabelecida a planilha de controle referenciada no Quadro 2, onde as recomendações da ISA 99 são tratadas. Observa-se que a tecnologia sugerida pela norma de segurança é descrita, e as vulnerabilidades associadas, deficiências e as recomendações são expostas.

Quadro 2 – Recomendações da ISA 99.

TECNOLOGIA	DESCRIÇÃO	VULNERABILIDADES CORRIGIDAS	DEFICIÊNCIAS	RECOMENDAÇÕES
<i>Virtual Networks (Vlan)</i>	Segmentação das redes físicas em redes lógicas	Segregação de tráfego	<i>Spoof Mac</i> <i>Spanning tree protocols</i> <i>VLAN Hopping</i>	Atualizações periódicas da versão; Segmentação da rede corporativa da industrial.
<i>Network Firewalls</i>	Mecanismo utilizado para controle de tráfego	Proteção das redes que passam pelo dispositivo	Necessidade de trabalhar em conjunto com detectores de intrusão; Grande quantidade de logs; Profissionais capacitados para as operações diárias.	Segmentação das redes em zonas; Criação de DMZ para tráfego internet.
<i>Virtual Private Network (VPN)</i>	Acesso remoto com criptografia	Acesso controlado a redes via autenticação	Acesso de qualquer lugar (internet) a rede corporativa	Método de autenticação forte
Utilitários de log de auditoria	Ferramenta de apoio de log	Checação de autenticação e utilização	Extensiva documentação e <i>backup</i>	Planejamento estratégico junto a outras áreas
<i>Biometric Authentication</i>	Autenticação biológica	Autenticação forte	Pouco utilizado	Utilização pontual em equipamentos restritos
Tecnologia de Autenticação e Autorização	Permissão e níveis de acesso	Acesso controlado a redes via autenticação	Necessidade de sincronização com todos os ativos do ambiente	Método de autenticação/autorização centralizada na rede
Criptografia	Processo de cifragem e decifragem	Criptografia em tráfego <i>clear text</i>	Deve-se utilizar um método de criptografia que todos os equipamentos suportem	Uso de criptografia em toda comunicação interna e externa
Detectores de Intrusão	Utilitário para detecção de eventos não permitidos na rede	Identificação de tráfego malicioso	Requer atualização de assinaturas e excesso de falso-positivo	Utilização em segmentos
Controle Físico	Acesso restrito aos equipamentos de campo	Somente pessoas autorizadas podem manipular e realizar alterações físicas	Se não utilizada com um método de biometria, pode mostrar ineficaz	Acesso controlado

Passo 6: Após a implantação dos controles é necessário um mecanismo de acompanhamento para evitar ocorrências desnecessárias. A implantação de controle pode ser realizada por meio de *softwares* de monitoração e emissão de relatórios periódicos.

Passo 7: A auditoria deve verificar se as condições de segurança da informação foram implantadas e documentadas de forma correta e conforme a política de segurança definida. As normas ISA 99 não tratam de auditoria, porém se faz necessário um mecanismo para detecção de não conformidades e ações preventivas para que os desvios identificados não ocorram mais. Dessa forma se faz necessário a realização periódica de auditorias internas e adicionalmente de auditoria externas para uma verificação mais precisa se a política de segurança definida está sendo seguida de maneira correta. De forma complementar, no próximo item é descrito um mecanismo auxiliar para detecção de eventos baseado no comportamento da estação de tratamento de água e que pode ser utilizado de forma complementar na auditoria.

Para criação do índice de criticidade, foi considerada a tabela da metodologia GUT juntamente com as recomendações da ISA 99, a qual gerou a Tabela 5.

Tabela 5 – Índice de criticidade.

PONTUAÇÃO	SITUAÇÃO	ÍNDICE
100-125	Extremamente grave	4
75-100	Muito grave	3
50-75	Grave	2
25-50	Pouco grave	1
0-25	Sem gravidade	0

Com a criação desse índice e juntamente com as definições das etapas anteriormente mencionadas, os cenários foram submetidos para avaliação. Para a coluna criticidade foram transportados os valores definidos pela metodologia GUT em conjunto com o índice de criticidade, o qual gerou o valor 22, tal valor é considerado como um índice seguro, conforme as definições e políticas de segurança da empresa. Todas as Plantas de saneamento submetidas devem chegar próximo desse valor para serem consideradas seguras. A coluna situação é a existência ou não de tal tecnologia, a existência é representada pelo número 1 e a inexistência pelo número 0.

No caso da inexistência da tecnologia o valor atribuído à criticidade será subtraído; ficando a fórmula abaixo responsável pelo valor final.

$$\text{Valor} = (\text{Soma da Criticidade} - (\text{Valor da Criticidade se Situação}=0))$$

CENÁRIO 1 – CAPITAL

Para o primeiro cenário, denominado Cenário 1 – Capital, a Planta de segurança é considerada segura, pois somente o IDS não estava presente na Planta da empresa, conforme ilustra a Tabela 6. Porém o valor desse item não foi considerado como prioritário pela definição da política de segurança da empresa e dessa forma não afetaram o índice de segurança. Mas de forma adicional é extremamente recomendada a aquisição de um detector de intrusão, bem como a realização de seu posicionamento de forma estratégica para visualização do tráfego interno e externo.

Tabela 6 – Índice da Planta Capital.

TECNOLOGIA	CRITICIDADE	SITUAÇÃO
<i>Firewall</i>	4	1
<i>Firewall</i> com redundância	1	1
Equipamentos com autenticação	4	1
Criptografia	1	1
Criptografia forte	0	1
IDS	2	0
Equipamentos atualizados	4	1
<i>Virtual Private Network</i>	0	1
Monitoração	1	1
Controle de acesso físico	3	1
Atualizações periódicas	1	1
<i>Virtual Local Network</i>	1	1
Total	22	20

CENÁRIO 2 – INTERIOR

Já para o segundo cenário, denominado Interior, a Planta de saneamento não foi considerada segura e revelou uma série de problemas, como ausência de *firewall*,

VPN e vlans. Portanto é extremamente recomendado que seja realizada uma análise mais específica na Planta de saneamento do Interior para que as tecnologias de segurança descritas nas normas ISA 99 sejam adotadas e utilizadas da melhor maneira possível. Adicionalmente, a Planta de saneamento, denominada Capital, pode ser utilizada como referencial para implantação das tecnologias. Na Tabela 7, é possível visualizar os itens não contemplados na Planta.

Tabela 7 – Índice da Planta Interior.

TECNOLOGIA	CRITICIDADE	SITUAÇÃO
<i>Firewall</i>	4	0
<i>Firewall</i> com redundância	1	0
Equipamentos com autenticação	4	0
Criptografia	1	1
Criptografia forte	0	0
IDS	2	0
Equipamentos atualizados	4	1
<i>Virtual Private Network</i>	0	0
Monitoração	1	1
Controle de acesso físico	3	1
Atualizações periódicas	1	1
<i>Virtual Local Network</i>	1	0
Total	22	10

CENÁRIO 3 – LITORAL

O terceiro, e último cenário, denominado Litoral, apresenta um equilíbrio na utilização dos recursos, porém não pode ser considerado extremamente seguro pois alguns itens críticos para segurança não foram contemplados na implementação. Nesse sentido, é recomendado que seja realizada uma segmentação da rede (vlan) entre a rede corporativa e a industrial para evitar o tráfego desnecessário entre as redes e, por consequência, uma melhoria de desempenho. Da mesma forma, como recomendado anteriormente, a Planta de saneamento denominada Capital pode ser utilizada como referencial para implantação das tecnologias. Na Tabela 8, a seguir, é possível visualizar os itens não contemplados na Planta.

Tabela 8 – Índice da Planta Litoral.

TECNOLOGIA	CRITICIDADE	SITUAÇÃO
<i>Firewall</i>	4	1
<i>Firewall</i> com redundância	1	0
Equipamentos com autenticação	4	1
Criptografia	1	1
Criptografia forte	0	0
IDS	2	0
Equipamentos atualizados	4	1
<i>Virtual Private Network</i>	0	1
Monitoração	1	1
Controle de acesso físico	3	1
Atualizações periódicas	1	1
<i>Virtual Local Network</i>	1	0
Total	22	18

5 FERRAMENTAS E SIMULAÇÕES

Para análise de funcionalidade das técnicas de segurança sugeridas e implementadas foi elaborado um sistema de detecção de eventos, com o objetivo principal de identificar uma ação maliciosa ou indesejada na Planta de automação de tratamento de água. Para isso, conforme detalhado no capítulo 4, todo o fluxograma e as etapas no processo de tratamento de água foram estudadas e o seu comportamento analisado para que assim os eventos críticos pudessem ser mapeados. Sendo assim, com base nesses estudos, os eventos a seguir foram considerados críticos e poderiam de uma maneira geral comprometer o fornecimento de água potável:

- desligamento das duas bombas na captação da água bruta;
- transbordo de água do tanque que recebe a água tratada;
- dosagem excessiva de substâncias.

A análise do comportamento foi realizada por meio de uma ferramenta *open*, denominada *wireshark*, que funciona como um analisador de protocolo de rede. A utilização do analisador de protocolo se deu em decorrência da necessidade da captação do tráfego na rede para caracterização e verificação do comportamento do sistema de tratamento de água. O detector de intrusão foi posicionado no mesmo segmento de rede do sistema SCADA para que fosse possível a visualização do tráfego até o servidor. Na Figura 26 é possível observar de maneira detalhada o posicionamento do detector de intrusão.

Figura 26 – Posicionamento do detector.

Fonte: Próprio autor.

Após a geração de tráfego o detector de intrusão realiza uma classificação dos eventos, podendo ser classificado como:

- **Normal:** evento que não representa uma ameaça ao ambiente e trata-se de um evento conhecido;
- **Ataque:** evento que pode ser caracterizado como um dos 3 comportamentos definidos como crítico nas etapas do tratamento de água.
 - **Evento 1** – desligamento das duas bombas na captação da água bruta;
 - **Evento 2** – transbordo de água do tanque que recebe a água tratada;
 - **Evento 3** – dosagem excessiva de substâncias.

Na Figura 27, é possível observar essa classificação.

Figura 27 – Classificação do evento.

Fonte: Próprio autor.

Para a comunicação do PLC com o sistema desenvolvido foi utilizado um conversor serial para ethernet, mostrado na Figura 28, e a comunicação foi realizada através do protocolo OPC. Dessa forma o equipamento PLC comunica diretamente com o OPC Servidor e este por sua vez disponibiliza as informações para o OPC Cliente.

Figura 28 – Conversor serial para ethernet.

Fonte: Próprio autor.

Na Figura 29, a seguir, é possível observar a leitura das variáveis diretamente do PLC.

Figura 29 – OPC Cliente.

Fonte: Próprio autor.

Na Figura 30, a seguir, observa-se o sucesso da comunicação via TCP/IP do PCL com o sistema desenvolvido.

The screenshot shows the 'OPC Server' application window. The top menu bar includes 'File', 'Registration', 'PLCs', 'Run', 'DCOM', and 'Help'. Below the menu is a toolbar with various icons. The main window displays a table with columns: 'PLC Name', 'PLC Type', 'Unit ID', 'Enabled', and 'Communication Parameters'. The table lists several OPC Servers (e.g., OPCServer1, OPCServer1.M01, OPCServer1.M02, etc.) and their communication parameters. Below this, there is a log table with columns: 'Date', 'Time', and 'Event'. The log shows a series of events, primarily 'Added new item: OPCServer1.M01' through 'OPCServer1.M151', occurring at various times on 1/9/2010.

Date	Time	Event
1/9/2010	00:34:38	Added new item: OPCServer1.M01
1/9/2010	00:34:38	Added new item: OPCServer1.M05
1/9/2010	00:34:38	Added new item: OPCServer1.M02
1/9/2010	00:34:38	Added new item: OPCServer1.M03
1/9/2010	00:34:38	Added new item: OPCServer1.M04
1/9/2010	00:34:38	Added new item: OPCServer1.M07
1/9/2010	00:34:38	Added new item: OPCServer1.M08
1/9/2010	00:34:38	Added new item: OPCServer1.M09
1/9/2010	00:34:38	Added new item: OPCServer1.M10
1/9/2010	00:34:38	Added new item: OPCServer1.M11
1/9/2010	00:34:38	Added new item: OPCServer1.M12
1/9/2010	00:34:38	Added new item: OPCServer1.M13
1/9/2010	00:34:38	Added new item: OPCServer1.M14
1/9/2010	00:34:38	Added new item: OPCServer1.M15
1/9/2010	00:34:38	Added new item: OPCServer1.M16
1/9/2010	00:34:38	Added new item: OPCServer1.M17
1/9/2010	00:34:38	Added new item: OPCServer1.M18
1/9/2010	00:34:38	Added new item: OPCServer1.M19
1/9/2010	00:34:38	Added new item: OPCServer1.M20
1/9/2010	00:34:38	Added new item: OPCServer1.M21
1/9/2010	00:34:38	Added new item: OPCServer1.M22
1/9/2010	00:34:38	Added new item: OPCServer1.M23
1/9/2010	00:34:38	Added new item: OPCServer1.M24
1/9/2010	00:34:38	Added new item: OPCServer1.M25
1/9/2010	00:34:38	Added new item: OPCServer1.M26
1/9/2010	00:34:38	Added new item: OPCServer1.M27
1/9/2010	00:34:38	Added new item: OPCServer1.M28
1/9/2010	00:34:38	Added new item: OPCServer1.M29
1/9/2010	00:34:38	Added new item: OPCServer1.M30
1/9/2010	00:34:38	Added new item: OPCServer1.M31
1/9/2010	00:34:38	Added new item: OPCServer1.M32
1/9/2010	00:34:38	Added new item: OPCServer1.M33
1/9/2010	00:34:38	Added new item: OPCServer1.M34
1/9/2010	00:34:38	Added new item: OPCServer1.M35
1/9/2010	00:34:38	Added new item: OPCServer1.M36
1/9/2010	00:34:38	Added new item: OPCServer1.M37
1/9/2010	00:34:38	Added new item: OPCServer1.M38
1/9/2010	00:34:38	Added new item: OPCServer1.M39
1/9/2010	00:34:38	Added new item: OPCServer1.M40
1/9/2010	00:34:38	Added new item: OPCServer1.M41
1/9/2010	00:34:38	Added new item: OPCServer1.M42
1/9/2010	00:34:38	Added new item: OPCServer1.M43
1/9/2010	00:34:38	Added new item: OPCServer1.M44
1/9/2010	00:34:38	Added new item: OPCServer1.M45
1/9/2010	00:34:38	Added new item: OPCServer1.M46
1/9/2010	00:34:38	Added new item: OPCServer1.M47
1/9/2010	00:34:38	Added new item: OPCServer1.M48
1/9/2010	00:34:38	Added new item: OPCServer1.M49
1/9/2010	00:34:38	Added new item: OPCServer1.M50
1/9/2010	00:34:38	Added new item: OPCServer1.M51
1/9/2010	00:34:38	Added new item: OPCServer1.M52
1/9/2010	00:34:38	Added new item: OPCServer1.M53
1/9/2010	00:34:38	Added new item: OPCServer1.M54
1/9/2010	00:34:38	Added new item: OPCServer1.M55
1/9/2010	00:34:38	Added new item: OPCServer1.M56
1/9/2010	00:34:38	Added new item: OPCServer1.M57
1/9/2010	00:34:38	Added new item: OPCServer1.M58
1/9/2010	00:34:38	Added new item: OPCServer1.M59
1/9/2010	00:34:38	Added new item: OPCServer1.M60
1/9/2010	00:34:38	Added new item: OPCServer1.M61
1/9/2010	00:34:38	Added new item: OPCServer1.M62
1/9/2010	00:34:38	Added new item: OPCServer1.M63
1/9/2010	00:34:38	Added new item: OPCServer1.M64
1/9/2010	00:34:38	Added new item: OPCServer1.M65
1/9/2010	00:34:38	Added new item: OPCServer1.M66
1/9/2010	00:34:38	Added new item: OPCServer1.M67
1/9/2010	00:34:38	Added new item: OPCServer1.M68
1/9/2010	00:34:38	Added new item: OPCServer1.M69
1/9/2010	00:34:38	Added new item: OPCServer1.M70
1/9/2010	00:34:38	Added new item: OPCServer1.M71
1/9/2010	00:34:38	Added new item: OPCServer1.M72
1/9/2010	00:34:38	Added new item: OPCServer1.M73
1/9/2010	00:34:38	Added new item: OPCServer1.M74
1/9/2010	00:34:38	Added new item: OPCServer1.M75
1/9/2010	00:34:38	Added new item: OPCServer1.M76
1/9/2010	00:34:38	Added new item: OPCServer1.M77
1/9/2010	00:34:38	Added new item: OPCServer1.M78
1/9/2010	00:34:38	Added new item: OPCServer1.M79
1/9/2010	00:34:38	Added new item: OPCServer1.M80
1/9/2010	00:34:38	Added new item: OPCServer1.M81
1/9/2010	00:34:38	Added new item: OPCServer1.M82
1/9/2010	00:34:38	Added new item: OPCServer1.M83
1/9/2010	00:34:38	Added new item: OPCServer1.M84
1/9/2010	00:34:38	Added new item: OPCServer1.M85
1/9/2010	00:34:38	Added new item: OPCServer1.M86
1/9/2010	00:34:38	Added new item: OPCServer1.M87
1/9/2010	00:34:38	Added new item: OPCServer1.M88
1/9/2010	00:34:38	Added new item: OPCServer1.M89
1/9/2010	00:34:38	Added new item: OPCServer1.M90
1/9/2010	00:34:38	Added new item: OPCServer1.M91
1/9/2010	00:34:38	Added new item: OPCServer1.M92
1/9/2010	00:34:38	Added new item: OPCServer1.M93
1/9/2010	00:34:38	Added new item: OPCServer1.M94
1/9/2010	00:34:38	Added new item: OPCServer1.M95
1/9/2010	00:34:38	Added new item: OPCServer1.M96
1/9/2010	00:34:38	Added new item: OPCServer1.M97
1/9/2010	00:34:38	Added new item: OPCServer1.M98
1/9/2010	00:34:38	Added new item: OPCServer1.M99
1/9/2010	00:34:38	Added new item: OPCServer1.M100
1/9/2010	00:34:38	Added new item: OPCServer1.M101
1/9/2010	00:34:38	Added new item: OPCServer1.M102
1/9/2010	00:34:38	Added new item: OPCServer1.M103
1/9/2010	00:34:38	Added new item: OPCServer1.M104
1/9/2010	00:34:38	Added new item: OPCServer1.M105
1/9/2010	00:34:38	Added new item: OPCServer1.M106
1/9/2010	00:34:38	Added new item: OPCServer1.M107
1/9/2010	00:34:38	Added new item: OPCServer1.M108
1/9/2010	00:34:38	Added new item: OPCServer1.M109
1/9/2010	00:34:38	Added new item: OPCServer1.M110
1/9/2010	00:34:38	Added new item: OPCServer1.M111
1/9/2010	00:34:38	Added new item: OPCServer1.M112
1/9/2010	00:34:38	Added new item: OPCServer1.M113
1/9/2010	00:34:38	Added new item: OPCServer1.M114
1/9/2010	00:34:38	Added new item: OPCServer1.M115
1/9/2010	00:34:38	Added new item: OPCServer1.M116
1/9/2010	00:34:38	Added new item: OPCServer1.M117
1/9/2010	00:34:38	Added new item: OPCServer1.M118
1/9/2010	00:34:38	Added new item: OPCServer1.M119
1/9/2010	00:34:38	Added new item: OPCServer1.M120
1/9/2010	00:34:38	Added new item: OPCServer1.M121
1/9/2010	00:34:38	Added new item: OPCServer1.M122
1/9/2010	00:34:38	Added new item: OPCServer1.M123
1/9/2010	00:34:38	Added new item: OPCServer1.M124
1/9/2010	00:34:38	Added new item: OPCServer1.M125
1/9/2010	00:34:38	Added new item: OPCServer1.M126
1/9/2010	00:34:38	Added new item: OPCServer1.M127
1/9/2010	00:34:38	Added new item: OPCServer1.M128
1/9/2010	00:34:38	Added new item: OPCServer1.M129
1/9/2010	00:34:38	Added new item: OPCServer1.M130
1/9/2010	00:34:38	Added new item: OPCServer1.M131
1/9/2010	00:34:38	Added new item: OPCServer1.M132
1/9/2010	00:34:38	Added new item: OPCServer1.M133
1/9/2010	00:34:38	Added new item: OPCServer1.M134
1/9/2010	00:34:38	Added new item: OPCServer1.M135
1/9/2010	00:34:38	Added new item: OPCServer1.M136
1/9/2010	00:34:38	Added new item: OPCServer1.M137
1/9/2010	00:34:38	Added new item: OPCServer1.M138
1/9/2010	00:34:38	Added new item: OPCServer1.M139
1/9/2010	00:34:38	Added new item: OPCServer1.M140
1/9/2010	00:34:38	Added new item: OPCServer1.M141
1/9/2010	00:34:38	Added new item: OPCServer1.M142
1/9/2010	00:34:38	Added new item: OPCServer1.M143
1/9/2010	00:34:38	Added new item: OPCServer1.M144
1/9/2010	00:34:38	Added new item: OPCServer1.M145
1/9/2010	00:34:38	Added new item: OPCServer1.M146
1/9/2010	00:34:38	Added new item: OPCServer1.M147
1/9/2010	00:34:38	Added new item: OPCServer1.M148
1/9/2010	00:34:38	Added new item: OPCServer1.M149
1/9/2010	00:34:38	Added new item: OPCServer1.M150
1/9/2010	00:34:38	Added new item: OPCServer1.M151

Figura 30 – OPC Servidor.

Fonte: Próprio autor.

Na Figura 31, é possível visualizar uma captura do tráfego de rede gerado entre o sistema de tratamento de água diretamente com o PLC.

The screenshot shows the Wireshark interface with a packet capture of network traffic. The packet list on the left shows several packets, with packet 55308 selected. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
55308	752.060961	192.168.127.254	192.168.127.253	TCP	complex-main > funk-logger [PSH, ACK] Seq=4082 Ack=6741 win=63081
55309	752.083653	192.168.127.254	192.168.127.253	TCP	complex-main > funk-logger [PSH, ACK] Seq=4086 Ack=6741 win=63081
55310	752.083769	192.168.127.253	192.168.127.254	TCP	funk-logger > complex-main [ACK] Seq=6741 Ack=4087 win=63081
55311	752.118769	192.168.127.253	192.168.127.254	TCP	funk-logger > complex-main [PSH, ACK] Seq=6741 Ack=4087 win=63081
55312	752.120858	192.168.127.254	192.168.127.253	TCP	complex-main > funk-logger [ACK] Seq=4087 Ack=6761 win=4076
55313	752.156908	192.168.127.254	192.168.127.253	TCP	complex-main > funk-logger [PSH, ACK] Seq=4087 Ack=6761 win=63081
55314	752.162966	192.168.127.254	192.168.127.253	TCP	complex-main > funk-logger [PSH, ACK] Seq=4091 Ack=6761 win=63081
55315	752.163686	192.168.127.253	192.168.127.254	TCP	funk-logger > complex-main [ACK] Seq=6761 Ack=4095 win=63073
55316	752.166636	192.168.127.254	192.168.127.253	TCP	complex-main > funk-logger [PSH, ACK] Seq=4095 Ack=6761 win=63081
55317	752.171903	192.168.127.254	192.168.127.253	TCP	complex-main > funk-logger [PSH, ACK] Seq=4099 Ack=6761 win=63081
55318	752.172007	192.168.127.253	192.168.127.254	TCP	funk-logger > complex-main [ACK] Seq=6761 Ack=4100 win=63068
55319	752.190174	192.168.127.253	192.168.127.254	TCP	funk-logger > complex-main [PSH, ACK] Seq=6761 Ack=4100 win=63068
55320	752.192102	192.168.127.254	192.168.127.253	TCP	complex-main > funk-logger [ACK] Seq=4100 Ack=6781 win=4076
55321	752.221223	192.168.127.254	192.168.127.253	TCP	complex-main > funk-logger [PSH, ACK] Seq=4100 Ack=6781 win=63068
55322	752.226198	192.168.127.254	192.168.127.253	TCP	complex-main > funk-logger [PSH, ACK] Seq=4104 Ack=6781 win=63068
55323	752.226323	192.168.127.253	192.168.127.254	TCP	funk-logger > complex-main [ACK] Seq=6781 Ack=4108 win=63060
55324	752.230453	192.168.127.254	192.168.127.253	TCP	complex-main > funk-logger [PSH, ACK] Seq=4108 Ack=6781 win=63068
55325	752.236443	192.168.127.254	192.168.127.253	TCP	complex-main > funk-logger [PSH, ACK] Seq=4112 Ack=6781 win=63068

Frame 55308 (60 bytes on wire, 60 bytes captured)

Ethernet II, Src: MoxaTech_16:7a:9c (00:90:e8:16:7a:9c), Dst: Vmware_6a:12:25 (00:0c:29:6a:12:25)

Internet Protocol, Src: 192.168.127.254 (192.168.127.254), Dst: 192.168.127.253 (192.168.127.253)

Transmission Control Protocol, Src Port: complex-main (5000), Dst Port: funk-logger (1786), Seq: 4082, Ack: 6741, Len: 4

Data (4 bytes)

```

0000  00 0c 29 6a 12 25 00 90  e8 16 7a 9c 08 00 45 00  ..j%. .z...E.
0010  00 2c 52 d2 00 00 3c 06  aa ad c0 a8 7f fe c0 a8  ..R...< .
0020  7f fd 13 88 06 fa 00 1f  1b 1d 02 4d 8a ea 50 18  .....M..P.
0030  10 00 d1 14 00 00 45 38  45 39 71 72  ....E8 E9qr

```

Figura 31 – Coleta de dados.

Fonte: Próprio autor.

Foi realizada a geração de tráfego para a comunicação do PLC com o sistema. Nessa geração de tráfego foram feitas simulações e entre elas os 3 eventos considerados como críticos são:

- **Evento 1** – desligamento das duas bombas na captação da água bruta;
- **Evento 2** – transbordo de água do tanque que recebe a água tratada;
- **Evento 3** – dosagem excessiva de substâncias.

5.1 SIMULAÇÃO 01 – DESLIGAMENTO DAS DUAS BOMBAS NA CAPTAÇÃO DA ÁGUA BRUTA

5.1.1 DESCRIÇÃO

Supõe-se que ocorreu o desligamento da bomba que realiza a captação da água bruta para a estação de tratamento de água. Esta situação pode ocorrer pelos motivos abaixo:

- Desligamento de forma acidental, ou seja, por erro do operador;
- Manutenção agendada;
- Evento inesperado.

A situação que pode ocorrer para o evento 1 é o desligamento das duas bombas de captação, de forma que o abastecimento de água em algumas horas pode parar, e, nesse caso, deve ser atendido pelos reservatórios espalhados estrategicamente ao longo da cidade. Esse evento somente poderá acontecer em situações controladas e de manutenção, porém segundo o ciclo de negócio identificado no estudo de campo é muito raro de acontecer. A situação mais comum é uma única bomba de captação trabalhar e, caso ocorra mudanças das características esperada da água, uma manobra para coleta de água do outro manancial é realizada. Sendo assim tem-se por premissa que o ambiente não está em estado de manutenção e está trabalhando dentro das suas características, ou seja, em alguns momentos uma bomba está trabalhando e outra não, e em outros momentos as bombas estão trabalhando de forma conjunta.

5.1.2 RESULTADO E ANÁLISE

A variável que identifica o funcionamento da bomba é MB0 e MB6; por tratar-se de uma operação booleana os valores possíveis são: 1, ou seja, em operação, e 0, inoperante.

Nesse sentido, as variáveis MB0 e MB6 podem estar alternando entre 1 e 0, porém nunca (somente em manutenção) trabalharam de forma zerada. Para identificação dessa ocorrência o detector de eventos deve verificar de forma constante as variáveis MB0 e MB6 e quando ambas estiverem zeradas um alerta enviado e uma mudança do valor da variável ocorrer.

Abaixo foi simulado no período de 08 horas o desligamento e ligamento das bombas de captação, sendo que no período das 4h às 6h ocorreu o desligamento de ambas as bombas, conforme evidência demonstrada no Gráfico 2. A variável MB0, responsável pela bomba primária, e a variável MB6, responsável pela bomba secundária, tiveram os valores zerados e identificados.

Gráfico 2 – Estado da bomba de captação.

Fonte: Próprio autor.

5.2 SIMULAÇÃO 02 – TRANSBORDO DE ÁGUA DO TANQUE QUE RECEBE A ÁGUA TRATADA

5.2.1 DESCRIÇÃO

Para o evento 2, observou-se que a variável MI0 é quem controla a capacidade de armazenamento do tanque. A alteração dessa variável, por meio da manipulação do pacote TCP/IP, pode ocorrer sem que necessariamente a capacidade do tanque esteja realmente cheia. Caso isso ocorra a bomba irá parar de funcionar e, conseqüentemente, em algumas horas o tanque estará vazio. Na Figura 32 é possível visualizar uma manipulação de variável. Dessa forma, para que esse evento não ocorra no ambiente, é necessário que o detector de eventos realize uma análise a cada hora para verificação de não ocorrência de uma mudança brusca nos valores da variável MI0.

Item	Datatype	Value	Startindex
OPCServer1.MI0	I2	30000	

Figura 32 – Manipulação de variável.

Fonte: Próprio autor.

5.2.2 RESULTADO E ANÁLISE

Para a simulação da manipulação dos parâmetros do estado do tanque, foram realizadas diversas interações manuais, alterando o valor da variável. Sendo que às 5h zerou-se o tanque, ou seja, o mesmo estava sem água, e posteriormente em outro momento das 7h às 8h ocorreu o transbordo do tanque, com valor acima de 30000. No Gráfico 3 é possível visualizar a detecção das interações realizadas.

Gráfico 3 – Estado da bomba de captação.
Fonte: Próprio autor.

5.3 SIMULAÇÃO 03 – DOSAGEM EXCESSIVA DE SUBSTÂNCIAS

5.3.1 DESCRIÇÃO

No evento 3, o controle da dosagem da substância soda cáustica é realizado por meio da variável MI21. O valor acordado e que não representa risco de envenenamento é de aproximadamente 19%. Sendo assim, caso ocorra uma dosagem excessiva, ou seja, além dos 19% acordados, um alerta para verificação da água deve ser emitido; de forma que a variável MI21 deve ser verificada constantemente e qualquer alteração de valor para maior de 19% representa um risco para a qualidade da água.

5.3.2 RESULTADO E ANÁLISE

Para simulação do controle de dosagem de substância no tanque utilizou-se o período de 12 horas, onde ocorreu um aumento gradativo da dosagem e

posteriormente, da mesma forma, uma redução na dosagem. As interações sempre ocorreram alterando o valor da variável MI21 de forma proposital. Foi detectado no período das 3h às 8h o aumento da dosagem da substância e posteriormente a normalização da mesma. No Gráfico 4 é possível visualizar o aumento das dosagens e depois a sua normalização.

Gráfico 4 – Controle de dosagem.

Fonte: Próprio autor.

6 CONCLUSÕES

Para a realização deste estudo foram realizadas diversas pesquisas bibliográficas atualizadas, abrangendo os mais variados temas da área de segurança da informação, com forte ênfase em sistemas industriais e redes industriais, além de um levantamento relacionado à segurança da informação no seu contexto global.

Primeiramente, é importante enfatizar que preparar uma metodologia para implementação segura em uma Planta de tratamento de água é uma tarefa complexa, tanto no nível técnico quanto no gerencial. Nessa perspectiva, são oferecidas uma abordagem e uma definição através de uma metodologia para implementação segura, partindo-se das necessidades da corporação.

O conjunto de normas de segurança ISA 99 fornece orientações para os elementos de segurança e gerenciamento, com o objetivo principal de obter conformidade para todos os elementos de segurança, contemplando conceitos básicos e estratégia, porém não cobre práticas, procedimentos e regras para aplicação ou a execução de uma implementação segura. Dessa forma o presente trabalho possibilitou a resolução dessa deficiência por meio de uma proposta de metodologia para implementação segura em Plantas de tratamento de água, que pode ser adaptada com modificações para outros tipos de sistemas industriais igualmente críticos.

A realização das etapas deste trabalho contribuiu para o conhecimento do comportamento de uma estação de tratamento de água, com as definições de fluxograma e todas as etapas que compõem o ciclo. O processo de caracterização permitiu o conhecimento dos equipamentos industriais e do sistema para realizar o controle e aquisição de dados, bem como os protocolos utilizados.

O desenvolvimento de um sistema para caracterização das etapas do tratamento de água possibilitou verificar o comportamento e os impactos na interação com os equipamentos da Planta industrial, além de poder ser utilizado na determinação de riscos no ambiente no qual esta inserido. Os experimentos realizados para verificar a detecção de eventos críticos mostraram-se adaptados ao ambiente e estão igualmente associados às etapas e ao conhecimento de todo o fluxo e da criticidade do processo. Os eventos considerados críticos foram detectados de

maneira esperada, conforme o negócio da empresa, porém uma abordagem real, e a utilização de alguma técnica de inteligência artificial, se faz necessário.

Por fim, a utilização de técnicas de segurança em conjunto com as normas ISA 99 apresentadas neste trabalho pode gerar benefícios no que tange à exposição de segurança e estender-se também com adaptações para outros ambientes igualmente críticos, tais como: fornecimento de energia, usina nuclear, petroquímica, entre outros.

6.1 TRABALHOS FUTUROS

A presente dissertação possibilita a realização dos seguintes trabalhos futuros:

1. O esquema de detecção de evento pode ser aperfeiçoado ou adaptado para outros ambientes;
2. Com a crescente utilização de técnicas de inteligência artificial, é possível usar uma destas técnicas para detecção e análise de anomalias no processo de tratamento de água;
3. O fluxograma e as etapas de tratamento de água podem ser reutilizados em trabalhos futuros. Ademais, pode-se realizar adaptações e aperfeiçoamentos na metodologia utilizada para o desenvolvimento desta dissertação;

REFERÊNCIAS

ALBUQUERQUE, P. U. B. D.; ALEXANDRIA, A. R. de. **Redes Industriais**: aplicações em sistemas digitais de controle distribuído. 2. ed. São Paulo: Ensino Profissional, 2009.

AMARAL FILHO, G. C. do. **Requisitos para sistemas de controle de sistemas produtivos integrados a gestão**. 2005. 194 p. Dissertação (Mestrado) – Escola Politécnica, Universidade de São Paulo, São Paulo, 2005.

ANDERSSON, R. **A method for assessment of system security**. Linköpings: Linköpings Universitet, 2005.

BACE, R.; MELL, P. **NIST special publication on intrusion detection systems**. Washington: National Institute of Standards and Technology – Computer Security Resource Center, 2001.

BAYBUTT, P. Sneak Path Security Analysis (SPSA) for Industrial cyber security. **Intech**, v. 51, n. 9, set. 2004.

BIGHAM, J.; GAMEZ, D.; LU, N. **Safeguarding SCADA systems with anomaly detection**. London: Department of Electronic Engineering, Queen Mary, University of London, 2003.

BYRES, E. J.; FRANZ, M.; MILLER, D. The use of attack trees in assessing vulnerabilities in SCADA systems. In: International Infrastructure Survivability Workshop (IISW'04), 2004, Lisbon. **Proceeding...** Lisbon: Institute of Electrical and Electronics Engineers, 2004.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.BR). **Estatísticas** mantidas pelo CERT.br. Disponível em: <<http://www.cert.br/stats/>>. Acesso em: 15 jan. 2010.

CHEBROLU, S.; ABRAHAM, A.; THOMAS, J. P. Feature deduction and ensemble design of intrusion detection systems. **Computers & Security**, p. 1-13, 2004.

CHESWICK, R. W.; BELLOVIN, M. S.; RUBIN, D. A. **Firewalls and internet security**. 2. ed. Boston: Pearson Education, 2003.

CHEUNG, S. et al. **Using model-based intrusion detection for SCADA networks**. Menlo Park, CA: Computer Science Laboratory, 2006.

COUTINHO, M. P. **Detecção de ataques em infra-estruturas críticas de sistemas elétricos de potência usando técnicas inteligentes**. 2007. Tese (Doutorado em Engenharia Elétrica) – Universidade Federal de Itajubá, Itajubá, 2007.

DNT. Governos de Estados Unidos e Coreia do Sul sofrem ataque organizado pela internet. Coreia do Norte é suspeita. **DNT**, 10 jul. 2009. Disponível em: <<http://www.dnt.adv.br/noticias/seguranca-da-informacao/governos-de-estados-unidos-e-coreia-do-sul-sofrem-ataque-organizado-pela-internet->>. Acesso em: 23 jul. 2010.

ESPINER, T. Georgia accuses Russia of coordinated cyberattack. **Cnet News**, 11 ago. 2008. Disponível em: <http://news.cnet.com/8301-1009_3-10014150-83.html>. Acesso em: 23 ago. 2010.

FERREIRA, A. B. D. H. **Novo Dicionário Aurélio da Língua Portuguesa**. 3. ed. Curitiba: Positivo, 2009.

FOLHA ONLINE. Presidente da Geórgia declara estado de guerra e pede cessar-fogo. **Folha.com**, 09 ago. 2008. Disponível em: <<http://www1.folha.uol.com.br/folha/mundo/ult94u431498.shtml>>. Acesso em: 23 ago. 2010.

HAMOUD, G.; CHEN, R.-L.; BRADLEY, I. Risk Assessment of Power Systems SCADA. In: Power Engineering Society General Meeting, 2003, Toronto, Canadá. **Proceeding...** Toronto, Canadá: IEE, 2003. 4 v.

JIN, X. et al. **Anomaly detection in electricity cyber infrastructures**. Disponível em: <www.davidgamez.eu/.../JinBighamRodawayGamezPhillips06_AnomalyDetectionElectricity.pdf>. Acesso em: 20 fev. 2010.

KRUTZ, R. L. **Securing Scada Systems**. Indianapolis: Wiley Publishing, Inc., 2006.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet**. São Paulo: Addison Wesley, 2003.

LIMNIOS, N. **Fault trees**: control systems, robotics & manufacturing series. [S.l.]: Wiley-ISTE, 2007.

MAFRA, P. M. et al. POLVO-IIDS: Um Sistema de Detecção de Intrusão Inteligente Baseado em Anomalias. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 8., 1-5 set. 2008, Gramado, RS. **Anais...** Gramado, RS: Sociedade Brasileira de Computação, 2008. p. 61-72.

MARCIANO, J. L. P. **Segurança da Informação**: uma abordagem social. 2006. 212 p. Tese (Doutorado em Ciências da Informação) – Universidade de Brasília, Brasília, 2006.

MARTINS, A. B.; SANTOS, C. A. S. Metodologia para implantação do sistema de gestão da segurança da informação. **Revista de Gestão da Tecnologia e Sistemas de Informação**, v. 2, n. 2, p. 121-136, 2005.

MCAFEE. **Virtual criminology report 2009**. Virtually here: the age of cyber warfare. [S.l.]: [s.n.], 2009.

MCMILLAN, R. Hackers break into water system network. **Computerworld**, 31 Oct. 2006. Disponível em: <http://www.computerworld.com/s/article/9004659/Hackers_break_into_water_system_network>. Acesso em: 03 set. 2010.

MORAES, C. C.; CASTRUCCI, P. D. L. **Engenharia de automação industrial**. Rio de Janeiro: LTC, 2007.

PALADY, P. **FMEA**: análise dos modos de falha e efeitos. 4. ed. São Paulo: Instituto IMAM, 2007.

POULSEN, K. Report: Cyber Attacks Caused Power Outages in Brazil. **Wired**, 7 nov. 2009. Disponível em: <<http://www.wired.com/threatlevel/2009/11/brazil>>. Acesso em: 23 ago. 2010.

RAMOS, A. **Guia oficial para formação de gestores em segurança**. São Paulo: Zouk, 2008.

SILVA, P. T.; CARVALHO, H.; TORRES, C. B. **Segurança dos sistemas de informação**: gestão estratégica da segurança empresarial. Lisboa: Centro Atlântico, 2003.

SOARES, L. F. G.; LEMOS, G.; COLCHER, S. **Redes de computadores das LANs MANs e WANs às Redes ATM**. 2. ed. Rio de Janeiro: Campus, 1995.

TANENBAUM, A. S. **Redes de computadores**. 4. ed. Rio de Janeiro: Elsevier, 2003.

TEIXEIRA, E. Uma guerra pela internet. **Veja Online**, 23 maio 2007. Disponível em: <http://veja.abril.com.br/230507/p_074.shtml>. Acesso em: 23 ago. 2010.

TORRES, J. M. **Analyzing risk and uncertainty for improving water distribution system security from malevolent water supply contamination events**. 2008. Thesis (Master's) – Office of Graduate Studies of Texas A&M University, Texas, 2008.

WILES, J. et al. **Techno security's guide to securing SCADA**: a comprehensive handbook on protecting the critical infrastructure. Burlington: Syngress, 2008.

BIBLIOGRAFIA

AXELSSON, S.; SANDS, D. **Understanding intrusion detection through visualization**. New York: Springer, 2006.

BARBOSA, A. H. **Detecção de intrusão em redes de automação industrial**. 2006. Dissertação (Mestrado em Informática) – Universidade Federal do Espírito Santo, Vitória, 2006.

BURBECK, K. **Adaptive real-time anomaly detection for safeguarding critical networks**. 2006. Thesis (Licentiate of Engineering) – Department of Computer and Information Science Linköpings Universitet, Linköping, Sweden, 2006.

BYRES, E.; LOWE, J. The myths and facts behind cyber security risks for industrial control systems. In: VDE Congress, 1-5 Oct. 2004, Berlin. **Proceeding...** Berlin: VDE, 2004.

COSTANTINI, K. C. **Development of a cyber attack simulator for network modeling and cyber security analysis**. 2007. Thesis (Master's) – Kate Gleason College of Engineering, Rochester Institute of Technology, New York, 2007.

FERNANDEZ, J. D.; FERNANDEZ, A. E. SCADA systems: vulnerabilities and remediation. **Journal of Computing Sciences in Colleges**, v. 20, n. 4, p. 160-168, 2005.

KOBAYASHI, T. H. **Uma ferramenta de manipulação de pacotes para análise de protocolos de redes industriais baseados em TCP/IP**. 2009. Dissertação (Mestrado) – Programa de Pós-Graduação em Engenharia Elétrica e de Computação, Universidade Federal do Rio Grande do Norte, Natal, 2009.

LIMA, I. V. M. **Uma abordagem simplificada de detecção de intrusão baseada em redes neurais artificiais**. 2005. Dissertação (Mestrado) – Sistema de Informação, Universidade Federal de Santa Catarina, Florianópolis, 2005.

LIU, Q.; LI, Y. Modbus/TCP based Network Control System for Water Process in the Firepower Plant. In: World Congress on Intelligent Control and Automation, 6., 21-23 June 2006, Dalian, China. **Proceeding...** Dalian, China: WCICA, 2006. p. 432-435.

MCAFEE. **In the crossfire**: critical infrastructure in the age of cyber war. [S.l.]: [s.n.], 2010.

SANTOS, R. D. O. **Segurança da informação em redes industriais**: ambiente para simulação e desenvolvimento de ferramentas. 2006. Monografia (Graduação em Ciências da Computação) – Universidade Federal do Espírito Santo, Vitória, 2006.

SCARFONE, K.; MELL, P. **Guide to intrusion detection and prevention systems (IDPS)**. Washington: NIST, 2007.

STAMP, J. et al. **Sustainable security for infrastructure SCADA**. Albuquerque, NM: Sandia National Laboratories, 2003.

TSANG, C.-H.; KWONG, S. Multi-Agent Intrusion Detection System in Industrial Network using Ant Colony Clustering Approach and Unsupervised Feature Extraction. In: Industrial Technology, 2005, Kowloon, Hong Kong. **Proceeding...** Kowloon, Hong Kong: IEEE, 2005. p. 51-56.

WIBERG, K. C. **Identifying supervisory control and data acquisition (SCADA) systems on a network via remote reconnaissance**. 2006. Thesis (Master's) – Naval Postgraduate School, Monterey, California, 2006.

YANG, D.; USYNIN, A.; HINES, J. W. Anomaly-based intrusion detection for SCADA systems. In: Intl. Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies, 5., 2006, Albuquerque, NM. **Proceeding...** Albuquerque, NM: NPIC & HMIT, 2006.

APÊNDICES

APÊNDICE A – PUBLICAÇÕES

Durante o período da elaboração desta dissertação de mestrado, foram apresentadas as seguintes contribuições em conferências internacionais realizadas em: Portugal, Espanha, Estados Unidos e Alemanha, relatando os resultados e as pesquisas realizadas.

➤ PUBLICAÇÕES NO ANO DE 2009

AZEVEDO, T. M.; MARTINS, B. A.; KOFUJI, T. S.; VEIGA, Q. M. Detecção de intrusões baseado em anomalias em sistemas de tratamento de água utilizando técnicas de inteligência artificial. In: Conferência Ibérica de Sistemas e Tecnologias de Informação – CISTI 2009, 4., 17-20 jun. 2009, Póvoa de Varzim, Portugal. **Anais...** Póvoa de Varzim, Portugal: CISTI, 2009. (ISBN: 978-989-96247-1-9).

➤ PUBLICAÇÕES NO ANO DE 2010

MARTINS, B. A.; AZEVEDO, M. T.; KOFUJI, T. S.; VIANA. Instrumentation, SCADA, LIMS: Tools for efficient management the operational process of the water treatment. In: International Instrumentation Symposium, 56., 2010, Rochester, Estados Unidos. **Proceeding...** Rochester, Estados Unidos: International Instrumentation Symposium, 2010. (ISBN: 978-193-60074-2-4).

AZEVEDO, M. T.; KOFUJI, T. S. Detecção de Intrusões em redes Industriais Utilizando Técnicas de Inteligência Artificial. In: Conferencia Ibérica de Sistemas y Tecnologías de Información, 5., 2010, Santiago de Compostela,

Espanha. **Anais...** Santiago de Compostela, Espanha: Cisti, 2010. 2 v. p. 213-217. (ISBN: 978-989-96247-3-3).

AZEVEDO, M. T.; KOFUJI, T. S.; MARTINS, B. A.; MUZZI. A simplified approach to intrusion detection based on anomalies in control and data acquisition systems. In: IADIS International Conference Intelligent Systems and Agents, 2010, Freiburg, Germany. **Proceeding...** Freiburg, Germany: IADIS, 2010. (ISBN: 978-972-8939-23-6).

APÊNDICE B – PORTARIA Nº 518/GM, DE 25 DE MARÇO DE 2004

Estabelece os procedimentos e responsabilidades relativos ao controle e vigilância da qualidade da água para consumo humano e seu padrão de potabilidade, e dá outras providências.

O MINISTRO DE ESTADO DA SAÚDE, INTERINO, no uso de suas atribuições e considerando o disposto no Art. 2º do Decreto nº 79.367, de 9 de março de 1977,

RESOLVE:

Art. 1º Aprovar a Norma de Qualidade da Água para Consumo Humano, na forma do Anexo desta Portaria, de uso obrigatório em todo território nacional.

Art. 2º Fica estabelecido o prazo máximo de 12 meses, contados a partir da publicação desta Portaria, para que as instituições ou órgãos aos quais esta Norma se aplica, promovam as adequações necessárias a seu cumprimento, no que se refere ao tratamento por filtração de água para consumo humano suprida por manancial superficial e distribuída por meio de canalização e da obrigação do monitoramento de cianobactérias e cianotoxinas.

Art. 3º É de responsabilidade da União, dos Estados, dos Municípios e do Distrito Federal a adoção das medidas necessárias para o fiel cumprimento desta Portaria.

Art. 4º O Ministério da Saúde promoverá, por intermédio da Secretaria de Vigilância em Saúde – SVS, a revisão da Norma de Qualidade da Água para Consumo Humano estabelecida nesta Portaria, no prazo de 5 anos ou a qualquer tempo, mediante solicitação devidamente justificada de órgãos governamentais ou não governamentais de reconhecida capacidade técnica nos setores objeto desta regulamentação.

Art. 5º Fica delegada competência ao Secretário de Vigilância em Saúde para editar, quando necessário, normas regulamentadoras desta Portaria.

Art. 6º Esta Portaria entra em vigor na data de sua publicação.

Art. 7º Fica revogada a Portaria nº 1469, de 29 de dezembro de 2000, publicada no DOU nº 1-E de 2 de janeiro de 2001, Seção 1, página nº 19.

GASTÃO WAGNER DE SOUSA CAMPOS

NORMA DE QUALIDADE DA ÁGUA PARA CONSUMO HUMANO

Capítulo I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Norma dispõe sobre procedimentos e responsabilidades inerentes ao controle e à vigilância da qualidade da água para consumo humano, estabelece seu padrão de potabilidade e dá outras providências.

Art. 2º Toda a água destinada ao consumo humano deve obedecer ao padrão de potabilidade e está sujeita à vigilância da qualidade da água.

Art. 3º Esta Norma não se aplica às águas envasadas e a outras, cujos usos e padrões de qualidade são estabelecidos em legislação específica.

Capítulo II

DAS DEFINIÇÕES

Art. 4º Para os fins a que se destina esta Norma, são adotadas as seguintes definições:

I - água potável – água para consumo humano cujos parâmetros microbiológicos, físicos, químicos e radioativos atendam ao padrão de potabilidade e que não ofereça riscos à saúde;

II - sistema de abastecimento de água para consumo humano – instalação composta por conjunto de obras civis, materiais e equipamentos, destinada à produção e à distribuição canalizada de água potável para populações, sob a responsabilidade do poder público, mesmo que administrada em regime de concessão ou permissão;

III - solução alternativa de abastecimento de água para consumo humano – toda modalidade de abastecimento coletivo de água distinta do sistema de abastecimento de água, incluindo, entre outras, fonte, poço comunitário, distribuição por veículo transportador, instalações condominiais horizontal e vertical;

IV - controle da qualidade da água para consumo humano – conjunto de atividades exercidas de forma contínua pelos responsáveis pela operação de sistema

ou solução alternativa de abastecimento de água, destinadas a verificar se a água fornecida à população é potável, assegurando a manutenção desta condição;

V - vigilância da qualidade da água para consumo humano – conjunto de ações adotadas continuamente pela autoridade de saúde pública, para verificar se a água consumida pela população atende à esta Norma e para avaliar os riscos que os sistemas e as soluções alternativas de abastecimento de água representam para a saúde humana;

VI - coliformes totais (bactérias do grupo coliforme) - bacilos gram-negativos, aeróbios ou anaeróbios facultativos, não formadores de esporos, oxidase-negativos, capazes de desenvolver na presença de sais biliares ou agentes tensoativos que fermentam a lactose com produção de ácido, gás e aldeído a $35,0 \pm 0,5^{\circ}\text{C}$ em 24-48 horas, e que podem apresentar atividade da enzima β -galactosidase. A maioria das bactérias do grupo coliforme pertence aos gêneros *Escherichia*, *Citrobacter*, *Klebsiella* e *Enterobacter*, embora vários outros gêneros e espécies pertençam ao grupo;

VII - coliformes termotolerantes - subgrupo das bactérias do grupo coliforme que fermentam a lactose a $44,5 \pm 0,2^{\circ}\text{C}$ em 24 horas; tendo como principal representante a *Escherichia coli*, de origem exclusivamente fecal;

VIII - *Escherichia Coli* - bactéria do grupo coliforme que fermenta a lactose e manitol, com produção de ácido e gás a $44,5 \pm 0,2^{\circ}\text{C}$ em 24 horas, produz indol a partir do triptofano, oxidase negativa, não hidroliza a uréia e apresenta atividade das enzimas β galactosidase e β glucoronidase, sendo considerada o mais específico indicador de contaminação fecal recente e de eventual presença de organismos patogênicos;

IX - contagem de bactérias heterotróficas - determinação da densidade de bactérias que são capazes de produzir unidades formadoras de colônias (UFC), na presença de compostos orgânicos contidos em meio de cultura apropriada, sob condições pré-estabelecidas de incubação: $35,0 \pm 0,5^{\circ}\text{C}$ por 48 horas;

X - cianobactérias - microorganismos procarióticos autotróficos, também denominados como cianofíceas (algas azuis), capazes de ocorrer em qualquer manancial superficial especialmente naqueles com elevados níveis de nutrientes (nitrogênio e fósforo), podendo produzir toxinas com efeitos adversos à saúde; e

XI - cianotoxinas - toxinas produzidas por cianobactérias que apresentam efeitos adversos à saúde por ingestão oral, incluindo:

a) microcistinas - hepatotoxinas heptapeptídicas cíclicas produzidas por cianobactérias, com efeito potente de inibição de proteínas fosfatases dos tipos 1 e 2A e promotoras de tumores;

b) cilindrospermopsina - alcalóide guanidínico cíclico produzido por cianobactérias, inibidor de síntese protéica, predominantemente hepatotóxico, apresentando também efeitos citotóxicos nos rins, baço, coração e outros órgãos; e

c) saxitoxinas - grupo de alcalóides carbamatos neurotóxicos produzido por cianobactérias, não sulfatados (saxitoxinas) ou sulfatados (goniautoxinas e C-toxinas) e derivados decarbamil, apresentando efeitos de inibição da condução nervosa por bloqueio dos canais de sódio.

Capítulo III

DOS DEVERES E DAS RESPONSABILIDADES

Seção I

Do Nível Federal

Art. 5º São deveres e obrigações do Ministério da Saúde, por intermédio da Secretaria de Vigilância em Saúde - SVS:

I. - promover e acompanhar a vigilância da qualidade da água, em articulação com as Secretarias de Saúde dos Estados e do Distrito Federal e com os responsáveis pelo controle de qualidade da água, nos termos da legislação que regulamenta o SUS;

II - estabelecer as referências laboratoriais nacionais e regionais, para dar suporte às ações de maior complexidade na vigilância da qualidade da água para consumo humano;

III - aprovar e registrar as metodologias não contempladas nas referências citadas no artigo 17 desta Norma;

IV - definir diretrizes específicas para o estabelecimento de um plano de amostragem a ser implementado pelos Estados, Distrito Federal ou Municípios, no exercício das atividades de vigilância da qualidade da água, no âmbito do Sistema Único de Saúde – SUS; e

V - executar ações de vigilância da qualidade da água, de forma complementar, em caráter excepcional, quando constatada, tecnicamente, insuficiência da ação estadual, nos termos da regulamentação do SUS.

Seção II

Do Nível Estadual e Distrito Federal

Art. 6º São deveres e obrigações das Secretarias de Saúde dos Estados e do Distrito Federal:

I - promover e acompanhar a vigilância da qualidade da água em sua área de competência, em articulação com o nível municipal e os responsáveis pelo controle de qualidade da água, nos termos da legislação que regulamenta o SUS;

II - garantir, nas atividades de vigilância da qualidade da água, a implementação de um plano de amostragem pelos municípios, observadas as diretrizes específicas a serem elaboradas pela SVS/MS;

III - estabelecer as referências laboratoriais estaduais e do Distrito Federal para dar suporte às ações de vigilância da qualidade da água para consumo humano; e

IV - executar ações de vigilância da qualidade da água, de forma complementar, em caráter excepcional, quando constatada, tecnicamente, insuficiência da ação municipal, nos termos da regulamentação do SUS.

Seção III

Do Nível Municipal

Art. 7º São deveres e obrigações das Secretarias Municipais de Saúde:

I - exercer a vigilância da qualidade da água em sua área de competência, em articulação com os responsáveis pelo controle de qualidade da água, de acordo com as diretrizes do SUS;

II - sistematizar e interpretar os dados gerados pelo responsável pela operação do sistema ou solução alternativa de abastecimento de água, assim como, pelos órgãos ambientais e gestores de recursos hídricos, em relação às características da água nos mananciais, sob a perspectiva da vulnerabilidade do abastecimento de água quanto aos riscos à saúde da população;

III - estabelecer as referências laboratoriais municipais para dar suporte às ações de vigilância da qualidade da água para consumo humano;

IV - efetuar, sistemática e permanentemente, avaliação de risco à saúde humana de cada sistema de abastecimento ou solução alternativa, por meio de informações sobre:

a) a ocupação da bacia contribuinte ao manancial e o histórico das características de suas águas;

b) as características físicas dos sistemas, práticas operacionais e de controle da qualidade da água;

c) o histórico da qualidade da água produzida e distribuída; e

d) a associação entre agravos à saúde e situações de vulnerabilidade do sistema.

V - auditar o controle da qualidade da água produzida e distribuída e as práticas operacionais adotadas;

VI - garantir à população informações sobre a qualidade da água e riscos à saúde associados, nos termos do inciso VI do artigo 9 desta Norma;

VII - manter registros atualizados sobre as características da água distribuída, sistematizados de forma compreensível à população e disponibilizados para pronto acesso e consulta pública;

VIII - manter mecanismos para recebimento de queixas referentes às características da água e para a adoção das providências pertinentes;

IX - informar ao responsável pelo fornecimento de água para consumo humano sobre anomalias e não conformidades detectadas, exigindo as providências para as correções que se fizerem necessárias;

X - aprovar o plano de amostragem apresentado pelos responsáveis pelo controle da qualidade da água de sistema ou solução alternativa de abastecimento de água, que deve respeitar os planos mínimos de amostragem expressos nas Tabelas 6, 7, 8 e 9;

XI - implementar um plano próprio de amostragem de vigilância da qualidade da água, consoante diretrizes específicas elaboradas pela SVS; e

XII - definir o responsável pelo controle da qualidade da água de solução alternativa.

Seção IV

Do Responsável pela Operação de Sistema e/ou Solução Alternativa

Art. 8º Cabe aos responsáveis pela operação de sistema ou solução alternativa de abastecimento de água, exercer o controle da qualidade da água.

Parágrafo único. Em caso de administração, em regime de concessão ou permissão do sistema de abastecimento de água, é a concessionária ou a permissionária a responsável pelo controle da qualidade da água.

Art. 9º Aos responsáveis pela operação de sistema de abastecimento de água incumbe:

I - operar e manter sistema de abastecimento de água potável para a população consumidora, em conformidade com as normas técnicas aplicáveis publicadas pela ABNT - Associação Brasileira de Normas Técnicas e com outras normas e legislações pertinentes;

II - manter e controlar a qualidade da água produzida e distribuída, por meio de:

a) controle operacional das unidades de captação, adução, tratamento, reservação e distribuição;

b) exigência do controle de qualidade, por parte dos fabricantes de produtos químicos utilizados no tratamento da água e de materiais empregados na produção e distribuição que tenham contato com a água;

c) capacitação e atualização técnica dos profissionais encarregados da operação do sistema e do controle da qualidade da água; e

d) análises laboratoriais da água, em amostras provenientes das diversas partes que compõem o sistema de abastecimento.

III - manter avaliação sistemática do sistema de abastecimento de água, sob a perspectiva dos riscos à saúde, com base na ocupação da bacia contribuinte ao manancial, no histórico das características de suas águas, nas características físicas do sistema, nas práticas operacionais e na qualidade da água distribuída;

IV - encaminhar à autoridade de saúde pública, para fins de comprovação do atendimento a esta Norma, relatórios mensais com informações sobre o controle da qualidade da água, segundo modelo estabelecido pela referida autoridade;

V - promover, em conjunto com os órgãos ambientais e gestores de recursos hídricos, as ações cabíveis para a proteção do manancial de abastecimento e de sua bacia contribuinte, assim como efetuar controle das características das suas águas,

nos termos do artigo 19 desta Norma, notificando imediatamente a autoridade de saúde pública sempre que houver indícios de risco à saúde ou sempre que amostras coletadas apresentarem resultados em desacordo com os limites ou condições da respectiva classe de enquadramento, conforme definido na legislação específica vigente;

VI - fornecer a todos os consumidores, nos termos do Código de Defesa do Consumidor, informações sobre a qualidade da água distribuída, mediante envio de relatório, dentre outros mecanismos, com periodicidade mínima anual e contendo, no mínimo, as seguintes informações:

a) descrição dos mananciais de abastecimento, incluindo informações sobre sua proteção, disponibilidade e qualidade da água;

b) estatística descritiva dos valores de parâmetros de qualidade detectados na água, seu significado, origem e efeitos sobre a saúde; e

c) ocorrência de não conformidades com o padrão de potabilidade e as medidas corretivas providenciadas.

VII - manter registros atualizados sobre as características da água distribuída, sistematizados de forma compreensível aos consumidores e disponibilizados para pronto acesso e consulta pública;

VIII - comunicar, imediatamente, à autoridade de saúde pública e informar, adequadamente, à população a detecção de qualquer anomalia operacional no sistema ou não conformidade na qualidade da água tratada, identificada como de risco à saúde, adotando-se as medidas previstas no artigo 29 desta Norma; e

IX - manter mecanismos para recebimento de queixas referentes às características da água e para a adoção das providências pertinentes.

Art. 10. Ao responsável por solução alternativa de abastecimento de água, nos termos do inciso XII do artigo 7 desta Norma, incumbe:

I - requerer, junto à autoridade de saúde pública, autorização para o fornecimento de água apresentando laudo sobre a análise da água a ser fornecida, incluindo os parâmetros de qualidade previstos nesta Portaria, definidos por critério da referida autoridade;

II - operar e manter solução alternativa que forneça água potável em conformidade com as normas técnicas aplicáveis, publicadas pela ABNT - Associação Brasileira de Normas Técnicas, e com outras normas e legislações pertinentes;

III - manter e controlar a qualidade da água produzida e distribuída, por meio de análises laboratoriais, nos termos desta Portaria e, a critério da autoridade de saúde pública, de outras medidas conforme inciso II do artigo anterior;

IV - encaminhar à autoridade de saúde pública, para fins de comprovação, relatórios com informações sobre o controle da qualidade da água, segundo modelo e periodicidade estabelecidos pela referida autoridade, sendo no mínimo trimestral;

V - efetuar controle das características da água da fonte de abastecimento, nos termos do artigo 19 desta Norma, notificando, imediatamente, à autoridade de saúde pública sempre que houver indícios de risco à saúde ou sempre que amostras coletadas apresentarem resultados em desacordo com os limites ou condições da respectiva classe de enquadramento, conforme definido na legislação específica vigente;

VI - manter registros atualizados sobre as características da água distribuída, sistematizados de forma compreensível aos consumidores e disponibilizados para pronto acesso e consulta pública;

VII - comunicar, imediatamente, à autoridade de saúde pública competente e informar, adequadamente, à população a detecção de qualquer anomalia identificada como de risco à saúde, adotando-se as medidas previstas no artigo 29; e

VIII - manter mecanismos para recebimento de queixas referentes às características da água e para a adoção das providências pertinentes.

Capítulo IV DO PADRÃO DE POTABILIDADE

Art. 11. A água potável deve estar em conformidade com o padrão microbiológico conforme Tabela 1, a seguir:

Tabela 1

Padrão microbiológico de potabilidade da água para consumo humano

PARÂMETRO	VMP ⁽¹⁾
Água para consumo humano ⁽²⁾	
Escherichia coli ou coliformes termotolerantes ⁽³⁾	Ausência em 100ml
Água na saída do tratamento	
Coliformes totais	Ausência em 100ml

Água tratada no sistema de distribuição (reservatórios e rede)	
Escherichia coli ou coliformes termotolerantes ⁽³⁾	Ausência em 100ml
Coliformes totais	<p>Sistemas que analisam 40 ou mais amostras por mês: Ausência em 100ml em 95% das amostras examinadas no mês;</p> <p>Sistemas que analisam menos de 40 amostras por mês: Apenas uma amostra poderá apresentar mensalmente resultado positivo em 100ml</p>

NOTAS:

(1) Valor Máximo Permitido.

(2) água para consumo humano em toda e qualquer situação, incluindo fontes individuais como poços, minas, nascentes, dentre outras.

(3) a detecção de Escherichia coli deve ser preferencialmente adotada.

§ 1º No controle da qualidade da água, quando forem detectadas amostras com resultado positivo para coliformes totais, mesmo em ensaios presuntivos, novas amostras devem ser coletadas em dias imediatamente sucessivos até que as novas amostras revelem resultado satisfatório.

§ 2º Nos sistemas de distribuição, a coleta deve incluir, no mínimo, três amostras simultâneas, sendo uma no mesmo ponto e duas outras localizadas a montante e a jusante.

§ 3º Amostras com resultados positivos para coliformes totais devem ser analisadas para Escherichia coli e, ou, coliformes termotolerantes, devendo, neste caso, ser efetuada a verificação e confirmação dos resultados positivos.

§ 4º O percentual de amostras com resultado positivo de coliformes totais em relação ao total de amostras coletadas nos sistemas de distribuição deve ser calculado mensalmente, excluindo as amostras extras (coleta).

§ 5º O resultado negativo para coliformes totais das amostras extras (recoletas) não anula o resultado originalmente positivo no cálculo dos percentuais de amostras com resultado positivo.

§ 6º Na proporção de amostras com resultado positivo admitidas mensalmente para coliformes totais no sistema de distribuição, expressa na Tabela 1, não são tolerados resultados positivos que ocorram em coleta, nos termos do § 1º deste artigo.

§ 7º Em 20% das amostras mensais para análise de coliformes totais nos sistemas de distribuição, deve ser efetuada a contagem de bactérias heterotróficas e, uma vez excedidas 500 unidades formadoras de colônia (UFC) por ml, devem ser

providenciadas imediata coleta, inspeção local e, se constatada irregularidade, outras providências cabíveis.

§ 8º Em complementação, recomenda-se a inclusão de pesquisa de organismos patogênicos, com o objetivo de atingir, como meta, um padrão de ausência, dentre outros, de enterovírus, cistos de *Giardia* spp e oocistos de *Cryptosporidium* sp.

§ 9º Em amostras individuais procedentes de poços, fontes, nascentes e outras formas de abastecimento sem distribuição canalizada, tolera-se a presença de coliformes totais, na ausência de *Escherichia coli* e, ou, coliformes termotolerantes, nesta situação devendo ser investigada a origem da ocorrência, tomadas providências imediatas de caráter corretivo e preventivo e realizada nova análise de coliformes.

Art. 12. Para a garantia da qualidade microbiológica da água, em complementação às exigências relativas aos indicadores microbiológicos, deve ser observado o padrão de turbidez expresso na Tabela 2, abaixo:

Tabela 2

Padrão de turbidez para água pós-filtração ou pré-desinfecção

TRATAMENTO DA ÁGUA	VMP ⁽¹⁾
Desinfecção (água subterrânea)	1,0 UT ⁽²⁾ em 95% das amostras
Filtração rápida (tratamento completo ou filtração direta)	1,0 UT ⁽²⁾
Filtração lenta	2,0 UT ⁽²⁾ em 95% das amostras

NOTAS:

(1) Valor máximo permitido.

(2) Unidade de turbidez.

§ 1º Entre os 5% dos valores permitidos de turbidez superiores aos VMP estabelecidos na Tabela 2, o limite máximo para qualquer amostra pontual deve ser de 5,0 UT, assegurado, simultaneamente, o atendimento ao VMP de 5,0 UT em qualquer ponto da rede no sistema de distribuição.

§ 2º Com vistas a assegurar a adequada eficiência de remoção de enterovírus, cistos de *Giardia* spp e oocistos de *Cryptosporidium* sp., recomenda-se, enfaticamente, que, para a filtração rápida, se estabeleça como meta a obtenção de efluente filtrado com valores de turbidez inferiores a 0,5 UT em 95% dos dados mensais e nunca superiores a 5,0 UT.

§ 3º O atendimento ao percentual de aceitação do limite de turbidez, expresso na Tabela 2, deve ser verificado, mensalmente, com base em amostras no mínimo diárias para desinfecção ou filtração lenta e a cada quatro horas para filtração rápida, preferivelmente, em qualquer caso, no efluente individual de cada unidade de filtração.

Art. 13. Após a desinfecção, a água deve conter um teor mínimo de cloro residual livre de 0,5 mg/L, sendo obrigatória a manutenção de, no mínimo, 0,2 mg/L em qualquer ponto da rede de distribuição, recomendando-se que a cloração seja realizada em pH inferior a 8,0 e tempo de contato mínimo de 30 minutos.

Parágrafo único. Admite-se a utilização de outro agente desinfetante ou outra condição de operação do processo de desinfecção, desde que fique demonstrado pelo responsável pelo sistema de tratamento uma eficiência de inativação microbiológica equivalente à obtida com a condição definida neste artigo.

Art. 14. A água potável deve estar em conformidade com o padrão de substâncias químicas que representam risco para a saúde expresso na Tabela 3, a seguir:

Tabela 3

Padrão de potabilidade para substâncias químicas que representam risco à saúde

PARÂMETRO	Unidade	VMP ⁽¹⁾
INORGÂNICAS		
Antimônio	mg/L	0,005
Arsênio	mg/L	0,01
Bário	mg/L	0,7
Cádmio	mg/L	0,005
Cianeto	mg/L	0,07
Chumbo	mg/L	0,01
Cobre	mg/L	2
Cromo	mg/L	0,05
Fluoreto ⁽²⁾	mg/L	1,5
Mercurio	mg/L	0,001
Nitrato (como N)	mg/L	10
Nitrito (como N)	mg/L	1
Selênio	mg/L	0,01
ORGÂNICAS		
Acrilamida	µg/L	0,5
Benzeno	µg/L	5
Benzo[a]pireno	µg/L	0,7
Cloreto de Vinila	µg/L	5

1,2 Dicloroetano	µg/L	10
1,1 Dicloroetano	µg/L	30
Diclorometano	µg/L	20
Estireno	µg/L	20
Tetracloroeto de Carbono	µg/L	2
Tetracloroetano	µg/L	40
Triclorobenzenos	µg/L	20
Tricloroetano	µg/L	70
AGROTÓXICOS		
Alaclor	µg/L	20,0
Aldrin e Dieldrin	µg/L	0,03
Atrazina	µg/L	2
Bentazona	µg/L	300
Clordano (isômeros)	µg/L	0,2
2,4 D	µg/L	30
DDT (isômeros)	µg/L	2
Endossulfan	µg/L	20
Endrin	µg/L	0,6
Glifosato	µg/L	500
Heptacloro e Heptacloro epóxido	µg/L	0,03
Hexaclorobenzeno	µg/L	1
Lindano (g-BHC)	µg/L	2
Metolacloro	µg/L	10
Metoxicloro	µg/L	20
Molinato	µg/L	6
Pendimetalina	µg/L	20
Pentaclorofenol	µg/L	9
Permetrina	µg/L	20
Propanil	µg/L	20
Simazina	µg/L	2
Trifluralina	µg/L	20
CIANOTOXINAS		
Microcistinas ⁽³⁾	µg/L	1,0
DESINFETANTES E PRODUTOS SECUNDÁRIOS DA DESINFECÇÃO		
Bromato	mg/L	0,025
Clorito	mg/L	0,2
Cloro livre ⁽⁴⁾	mg/L	5
Monocloramina	mg/L	3
2,4,6 Triclorofenol	mg/L	0,2
Trihalometanos Total	mg/L	0,1

NOTAS:

(1) Valor Máximo Permitido.

(2) Os valores recomendados para a concentração de íon fluoreto devem observar à legislação específica vigente relativa à fluoretação da água, em qualquer caso devendo ser respeitado o VMP desta Tabela.

(3) É aceitável a concentração de até 10 µg/L de microcistinas em até 3 (três) amostras, consecutivas ou não, nas análises realizadas nos últimos 12 (doze) meses.

(4) Análise exigida de acordo com o desinfetante utilizado.

§ 1º Recomenda-se que as análises para cianotoxinas incluam a determinação de cilindrospermopsina e saxitoxinas (STX), observando, respectivamente, os valores limites de 15,0 µg/L e 3,0 µg/L de equivalentes STX/L.

§ 2º Para avaliar a presença dos inseticidas organofosforados e carbamatos na água, recomenda-se a determinação da atividade da enzima acetilcolinesterase, observando os limites máximos de 15% ou 20% de inibição enzimática, quando a enzima utilizada for proveniente de insetos ou mamíferos, respectivamente.

Art. 15. A água potável deve estar em conformidade com o padrão de radioatividade expresso na Tabela 4, a seguir:

Tabela 4

Padrão de radioatividade para água potável

Parâmetro	Unidade	VMP ⁽¹⁾
Radioatividade alfa global	Bq/L	0,1 ⁽²⁾
Radioatividade beta global	Bq/L	1,0 ⁽²⁾

NOTAS:

(1) Valor máximo permitido.

(2) Se os valores encontrados forem superiores aos VMP, deverá ser feita a identificação dos radionuclídeos presentes e a medida das concentrações respectivas. Nesses casos, deverão ser aplicados, para os radionuclídeos encontrados, os valores estabelecidos pela legislação pertinente da Comissão Nacional de Energia Nuclear - CNEN, para se concluir sobre a potabilidade da água.

Art. 16. A água potável deve estar em conformidade com o padrão de aceitação de consumo expresso na Tabela 5, a seguir:

Tabela 5

Padrão de aceitação para consumo humano

PARÂMETRO	Unidade	VMP ⁽¹⁾
Alumínio	mg/L	0,2
Amônia (como NH ₃)	mg/L	1,5
Cloreto	mg/L	250
Cor Aparente	uH ⁽²⁾	15
Dureza	mg/L	500
Etilbenzeno	mg/L	0,2
Ferro	mg/L	0,3
Manganês	mg/L	0,1

Monoclorobenzeno	mg/L	0,12
Odor	-	Não objetável ⁽³⁾
Gosto	-	Não objetável ⁽³⁾
Sódio	mg/L	200
Sólidos dissolvidos totais	mg/L	1.000
Sulfato	mg/L	250
Sulfeto de Hidrogênio	mg/L	0,05
Surfactantes	mg/L	0,5
Tolueno	mg/L	0,17
Turbidez	UT ⁽⁴⁾	5
Zinco	mg/L	5
Xileno	mg/L	0,3

NOTAS:

(1) Valor máximo permitido.

(2) Unidade Hazen (mg Pt–Co/L).

(3) critério de referência

(4) Unidade de turbidez.

§ 1º Recomenda-se que, no sistema de distribuição, o pH da água seja mantido na faixa de 6,0 a 9,5.

§ 2º Recomenda-se que o teor máximo de cloro residual livre, em qualquer ponto do sistema de abastecimento, seja de 2,0 mg/L.

§ 3º Recomenda-se a realização de testes para detecção de odor e gosto em amostras de água coletadas na saída do tratamento e na rede de distribuição de acordo com o plano mínimo de amostragem estabelecido para cor e turbidez nas Tabelas 6 e 7.

Art. 17. As metodologias analíticas para determinação dos parâmetros físicos, químicos, microbiológicos e de radioatividade devem atender às especificações das normas nacionais que disciplinem a matéria, da edição mais recente da publicação Standard Methods for the Examination of Water and Wastewater, de autoria das instituições American Public Health Association (APHA), American Water Works Association (AWWA) e Water Environment Federation (WEF), ou das normas publicadas pela ISO (International Standardization Organization).

§ 1º Para análise de cianobactérias e cianotoxinas e comprovação de toxicidade por bioensaios em camundongos, até o estabelecimento de especificações em normas nacionais ou internacionais que disciplinem a matéria, devem ser adotadas as metodologias propostas pela Organização Mundial da Saúde (OMS) em sua

publicação Toxic cyanobacteria in water: a guide to their public health consequences, monitoring and management.

§ 2º Metodologias não contempladas nas referências citadas no § 1º e “caput” deste artigo, aplicáveis aos parâmetros estabelecidos nesta Norma, devem, para ter validade, receber aprovação e registro pelo Ministério da Saúde.

§ 3º As análises laboratoriais para o controle e a vigilância da qualidade da água podem ser realizadas em laboratório próprio ou não que, em qualquer caso, deve manter programa de controle de qualidade interna ou externa ou ainda ser acreditado ou certificado por órgãos competentes para esse fim.

Capítulo V

DOS PLANOS DE AMOSTRAGEM

Art. 18. Os responsáveis pelo controle da qualidade da água de sistema ou solução alternativa de abastecimento de água devem elaborar e aprovar, junto à autoridade de saúde pública, o plano de amostragem de cada sistema, respeitando os planos mínimos de amostragem expressos nas Tabelas 6, 7, 8 e 9.

Tabela 6

Número mínimo de amostras para o controle da qualidade da água de sistema de abastecimento, para fins de análises físicas, químicas e de radioatividade, em função do ponto de amostragem, da população abastecida e do tipo de manancial

PARÂMETRO	TIPO DE MANANCIAL	SAÍDA DO TRATAMENTO (NÚMERO DE AMOSTRAS POR UNIDADE DE TRATAMENTO)	SISTEMA DE DISTRIBUIÇÃO (RESERVATÓRIOS E REDE)		
			População abastecida		
			< 50.000 hab.	0.000 a 250.000 hab.	> 250.000 hab.
Cor Turbidez pH	Superficial	1	10	5 para cada 5.000 hab.	40 + (1 para cada 25.000 hab.)
	Subterrâneo	1	5	1 para cada 1.000 hab.	20 + (1 para cada 50.000 hab.)

CRL ⁽¹⁾	Superficial	1	(Conforme § 3º do artigo 18).		
	Subterrâneo	1			
Fluoreto	Superficial ou Subterrâneo	1	5	1 para cada 1 000 hab.	20 + (1 para cada 50.000 hab.)
Cianotoxinas	Superficial	1 (Conforme § 5º do artigo 18)	-	-	-
Trihalometanos	Superficial	1	1 ⁽²⁾	4 ⁽²⁾	4 ⁽²⁾
	Subterrâneo	-	1 ⁽²⁾	1 ⁽²⁾	1 ⁽²⁾
Demais parâmetros ⁽³⁾	Superficial ou Subterrâneo	1	1 ⁽⁴⁾	1 ⁽⁴⁾	1 ⁽⁴⁾

NOTAS:

(1) Cloro residual livre.

(2) As amostras devem ser coletadas, preferencialmente, em pontos de maior tempo de detenção da água no sistema de distribuição.

(3) Apenas será exigida obrigatoriedade de investigação dos parâmetros radioativos quando da evidência de causas de radiação natural ou artificial.

(4) Dispensada análise na rede de distribuição quando o parâmetro não for detectado na saída do tratamento e, ou, no manancial, à exceção de substâncias que potencialmente possam ser introduzidas no sistema ao longo da distribuição.

Tabela 7

Frequência mínima de amostragem para o controle da qualidade da água de sistema de abastecimento, para fins de análises físicas, químicas e de radioatividade, em função do ponto de amostragem, da população abastecida e do tipo de manancial.

PARÂMETRO	TIPO DE MANANCIAL	SAÍDA DO TRATAMENTO (FREQUÊNCIA POR UNIDADE DE TRATAMENTO)	SISTEMA DE DISTRIBUIÇÃO (RESERVATÓRIOS E REDE)		
			População abastecida		
			<5 0.000 hab.	5 0.000 a 250.000 hab.	> 250.000 hab.
Cor					
Turbidez					
pH	Superficial	A cada 2 horas			
Fluoreto	Subterrâneo	Diária			
CRL ⁽¹⁾	Superficial	A cada 2 horas	(Conforme § 3º do artigo 18).		
	Subterrâneo	Diária			
Cianotoxinas	Superficial	Semanal (Conforme § 5º do artigo 18)	-	-	-
Trihalometanos	Superficial	Trimestral	Trimestral	Trimestral	Trimestral
	Subterrâneo	-	Anual	Semestral	Semestral

Demais parâmetros ⁽²⁾	Superficial ou Subterrâneo	Semestral	mestral ⁽³⁾	emestral ⁽³⁾	emestral ⁽³⁾
----------------------------------	----------------------------	-----------	------------------------	-------------------------	-------------------------

NOTAS:

(1) Cloro residual livre.

(2) Apenas será exigida obrigatoriedade de investigação dos parâmetros radioativos quando da evidência de causas de radiação natural ou artificial.

(3) Dispensada análise na rede de distribuição quando o parâmetro não for detectado na saída do tratamento e, ou, no manancial, à exceção de substâncias que potencialmente possam ser introduzidas no sistema ao longo da distribuição.

Tabela 8

Número mínimo de amostras mensais para o controle da qualidade da água de sistema de abastecimento, para fins de análises microbiológicas, em função da população abastecida.

PARÂMETRO	SISTEMA DE DISTRIBUIÇÃO (RESERVATÓRIOS E REDE)			
	População abastecida			
	< 5.000 hab.	5.000 a 20.000 hab.	20.000 a 250.000 hab.	> 250.000 hab.
Coliformes totais	1 0	1 para cada 500 hab.	30 + (1 para cada 2.000 hab.)	105 + (1 para cada 5.000 hab.) Máximo de 1.000

NOTA: na saída de cada unidade de tratamento devem ser coletadas, no mínimo, 2 (duas) amostras semanais, recomendando-se a coleta de, pelo menos, 4 (quatro) amostras semanais.

Tabela 9

Número mínimo de amostras e frequência mínima de amostragem para o controle da qualidade da água de solução alternativa, para fins de análises físicas, químicas e microbiológicas, em função do tipo de manancial e do ponto de amostragem.

PARÂMETRO	TIPO DE MANANCIAL	SAÍDA DO TRATAMENTO (para água canalizada)	NÚMERO DE AMOSTRAS RETIRADAS NO PONTO DE CONSUMO ⁽¹⁾ (para cada 500 hab.)	FREQÜÊNCIA DE AMOSTRAGEM
Cor, turbidez	Superficial	1	1	Semanal
pH e coliformes totais ⁽²⁾	Subterrâneo	1	1	Mensal
CRL ^{(2) (3)}	Superficial ou Subterrâneo	1	1	Diário

NOTAS:

(1) Devem ser retiradas amostras em, no mínimo, 3 pontos de consumo de água.

(2) Para veículos transportadores de água para consumo humano, deve ser realizada 1 (uma) análise de CRL em cada carga e 1 (uma) análise, na fonte de fornecimento, de cor, turbidez, PH e coliformes totais com frequência mensal, ou outra amostragem determinada pela autoridade de saúde pública.

(3) Cloro residual livre.

§ 1º A amostragem deve obedecer aos seguintes requisitos:

I - distribuição uniforme das coletas ao longo do período; e

II - representatividade dos pontos de coleta no sistema de distribuição (reservatórios e rede), combinando critérios de abrangência espacial e pontos estratégicos, entendidos como aqueles próximos a grande circulação de pessoas (terminais rodoviários, terminais ferroviários, etc.) ou edifícios que alberguem grupos populacionais de risco (hospitais, creches, asilos, etc.), aqueles localizados em trechos vulneráveis do sistema de distribuição (pontas de rede, pontos de queda de pressão, locais afetados por manobras, sujeitos à intermitência de abastecimento, reservatórios, etc.) e locais com sistemáticas notificações de agravos à saúde tendo como possíveis causas agentes de veiculação hídrica.

§ 2º No número mínimo de amostras coletadas na rede de distribuição, previsto na Tabela 8, não se incluem as amostras extras (recoletas).

§ 3º Em todas as amostras coletadas para análises microbiológicas deve ser efetuada, no momento da coleta, medição de cloro residual livre ou de outro composto residual ativo, caso o agente desinfetante utilizado não seja o cloro.

§ 4º Para uma melhor avaliação da qualidade da água distribuída, recomenda-se que, em todas as amostras referidas no § 3º deste artigo, seja efetuada a determinação de turbidez.

§ 5º Sempre que o número de cianobactérias na água do manancial, no ponto de captação, exceder 20.000 células/ml ($2\text{mm}^3/\text{L}$ de biovolume), durante o monitoramento que trata o § 1º do artigo 19, será exigida a análise semanal de cianotoxinas na água na saída do tratamento e nas entradas (hidrômetros) das clínicas de hemodiálise e indústrias de injetáveis, sendo que esta análise pode ser dispensada quando não houver comprovação de toxicidade na água bruta por meio da realização semanal de bioensaios em camundongos.

Art. 19. Os responsáveis pelo controle da qualidade da água de sistemas e de soluções alternativas de abastecimento supridos por manancial superficial devem coletar amostras semestrais da água bruta, junto do ponto de captação, para análise de acordo com os parâmetros exigidos na legislação vigente de classificação e enquadramento de águas superficiais, avaliando a compatibilidade entre as características da água bruta e o tipo de tratamento existente.

§ 1º O monitoramento de cianobactérias na água do manancial, no ponto de captação, deve obedecer frequência mensal, quando o número de cianobactérias não

exceder 10.000 células/ml (ou 1mm³/L de biovolume), e semanal, quando o número de cianobactérias exceder este valor.

§ 2º É vedado o uso de algicidas para o controle do crescimento de cianobactérias ou qualquer intervenção no manancial que provoque a lise das células desses microrganismos, quando a densidade das cianobactérias exceder 20.000 células/ml (ou 2mm³/L de biovolume), sob pena de comprometimento da avaliação de riscos à saúde associados às cianotoxinas.

Art. 20. A autoridade de saúde pública, no exercício das atividades de vigilância da qualidade da água, deve implementar um plano próprio de amostragem, consoante diretrizes específicas elaboradas no âmbito do Sistema Único de Saúde - SUS.

Capítulo VI

DAS EXIGÊNCIAS APLICÁVEIS AOS SISTEMAS E SOLUÇÕES ALTERNATIVAS DE ABASTECIMENTO DE ÁGUA

Art. 21. O sistema de abastecimento de água deve contar com responsável técnico, profissionalmente habilitado.

Art. 22. Toda água fornecida coletivamente deve ser submetida a processo de desinfecção, concebido e operado de forma a garantir o atendimento ao padrão microbiológico desta Norma.

Art. 23. Toda água para consumo humano suprida por manancial superficial e distribuída por meio de canalização deve incluir tratamento por filtração.

Art. 24. Em todos os momentos e em toda sua extensão, a rede de distribuição de água deve ser operada com pressão superior à atmosférica.

§ 1º Caso esta situação não seja observada, fica o responsável pela operação do serviço de abastecimento de água obrigado a notificar a autoridade de saúde pública e informar à população, identificando períodos e locais de ocorrência de pressão inferior à atmosférica.

§ 2º Excepcionalmente, caso o serviço de abastecimento de água necessite realizar programa de manobras na rede de distribuição, que possa submeter trechos a pressão inferior à atmosférica, o referido programa deve ser previamente comunicado à autoridade de saúde pública.

Art. 25. O responsável pelo fornecimento de água por meio de veículos deve:

- I - garantir o uso exclusivo do veículo para este fim;
 - II - manter registro com dados atualizados sobre o fornecedor e, ou, sobre a fonte de água; e
 - III - manter registro atualizado das análises de controle da qualidade da água.
- § 1º A água fornecida para consumo humano por meio de veículos deve conter um teor mínimo de cloro residual livre de 0,5 mg/L.
- § 2º O veículo utilizado para fornecimento de água deve conter, de forma visível, em sua carroceria, a inscrição: “ÁGUA POTÁVEL”.

Capítulo VII DAS PENALIDADES

Art. 26. Serão aplicadas as sanções administrativas cabíveis, aos responsáveis pela operação dos sistemas ou soluções alternativas de abastecimento de água, que não observarem as determinações constantes desta Portaria.

Art. 27. As Secretarias de Saúde dos Estados, do Distrito Federal e dos Municípios estarão sujeitas a suspensão de repasse de recursos do Ministério da Saúde e órgãos ligados, diante da inobservância do contido nesta Portaria.

Art. 28. Cabe ao Ministério da Saúde, por intermédio da SVS/MS, e às autoridades de saúde pública dos Estados, do Distrito Federal e dos Municípios, representadas pelas respectivas Secretarias de Saúde ou órgãos equivalentes, fazer observar o fiel cumprimento desta Norma, nos termos da legislação que regulamenta o Sistema Único de Saúde – SUS.

CAPÍTULO VIII DAS DISPOSIÇÕES FINAIS

Art. 29. Sempre que forem identificadas situações de risco à saúde, o responsável pela operação do sistema ou solução alternativa de abastecimento de água e as autoridades de saúde pública devem estabelecer entendimentos para a elaboração de um plano de ação e tomada das medidas cabíveis, incluindo a eficaz comunicação à população, sem prejuízo das providências imediatas para a correção da anormalidade.

Art. 30. O responsável pela operação do sistema ou solução alternativa de abastecimento de água pode solicitar à autoridade de saúde pública a alteração na frequência mínima de amostragem de determinados parâmetros estabelecidos nesta Norma.

Parágrafo único. Após avaliação criteriosa, fundamentada em inspeções sanitárias e, ou, em histórico mínimo de dois anos do controle e da vigilância da qualidade da água, a autoridade de saúde pública decidirá quanto ao deferimento da solicitação, mediante emissão de documento específico.

Art. 31. Em função de características não conformes com o padrão de potabilidade da água ou de outros fatores de risco, a autoridade de saúde pública competente, com fundamento em relatório técnico, determinará ao responsável pela operação do sistema ou solução alternativa de abastecimento de água que amplie o número mínimo de amostras, aumente a frequência de amostragem ou realize análises laboratoriais de parâmetros adicionais ao estabelecido na presente Norma.

Art. 32. Quando não existir na estrutura administrativa do Estado a unidade da Secretaria de Saúde, os deveres e responsabilidades previstos no artigo 6º desta Norma serão cumpridos pelo órgão equivalente.

APÊNDICE C – CÓDIGO FONTE DOS APLICATIVOS

PROJETO CONTROLE DE ÁGUA

➤ DESIGNER

➤ FRMSIMULADOR.CS

```

using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using Opc.Da;
using System.Collections;

namespace SumAguaEsgoto
{
    public partial class frmSimulador : Form
    {
        public static PSCollector OpcCollector;
        public static PSOPCServer OpcServer;
    }

```

```

public static PsTag[] SAEPSTags = null;
public static Hashtable SAETags = null;

private SubscriptionState opcSubscriptionState = new SubscriptionState();
private Opc.Da.Server opcServerConnection;
private Subscription opcSubscription;
private PSOPCServer opcServer;

private int iTQ1Nivel = 0;
private int iPumpIndex = 0;
private int iHelice = 0;
private int iStatusComunicacao = 0;

string sTQ1StatusMotor = "";
string sTQ1NivelMin = "";
string sTQ1NivelMax = "";
string sTQ1NivelReal = "";
string sFLStatusValvula = "";
string sFLNivelReal = "";
string sFLNivelMin = "";
string sFLNivelMax = "";
string sFILStatusValvula = "";
string sTQ2StatusValvula = "";
string sTQ2NivelReal = "";
string sTQ2NivelMin = "";
string sTQ2NivelMax = "";

//Tanque 3
string sTQ3StatusValvula = "";
string sTQ3NivelReal = "";
string sTQ3NivelMin = "";
string sTQ3NivelMax = "";

//Tanque 4
string sTQ4NivelReal = "";
string sTQ4NivelMin = "";
string sTQ4NivelMax = "";

//Dosagem Sulfato
string sSFStatusValvula = "";
string sSFSetPoint = "";
string sSFReal = "";

//Dosagem Soda
string sSDStatusValvula = "";
string sSDSetPoint = "";
string sSDReal = "";

//Dosagem Cloro
string sCLStatusValvula = "";

```

```

string sCLSetPoint = "";
string sCLReal = "";

//Dosagem Cloro TQ3
string sCLTQ3StatusValvula = "";
string sCLTQ3SetPoint = "";
string sCLTQ3Real = "";

//Dosagem Fluor TQ3
string sFLTQ3StatusValvula = "";
string sFLTQ3SetPoint = "";
string sFLTQ3Real = "";

//Tanque TQ5
string sTQ5StatusMotor = "";
string sConsumoAgua = "";

//Status do Tanque
string sStatusProcesso = "";

//Status Comunicação com o PLC
string sStatusPLC = "";

public frmSimulador()
{
    InitializeComponent();
}

/// <summary>
/// Load opc settings to read sensor
/// </summary>
private void LoadOPCSettings()
{
    try
    {
        tmrHelice.Start();
        tmrComunicacaoRede.Start();
        tmrStatusPLC.Start();

        //Start opc communication
        opcSubscriptionState.Name = "OPCServer1";
        opcSubscriptionState.Active = true;
        opcSubscriptionState.UpdateRate = 10;

        opcServer = Utils.GetOPCServer(OpcCollector.Hostname);
        opcServerConnection = opcServer.Connect();
        opcSubscription
(Opc.Da.Subscription)opcServerConnection.CreateSubscription(opcSubscriptionState)
;
    }
}

```

```

string[] aryltems = new string[] {

    "OPCServer1.MB100", //Liga/Desliga o Processo
    "OPCServer1.MB0", // Status Motor TQ1
    "OPCServer1.MI0", // Nível Real TQ1
    "OPCServer1.MI1", // SP Nível Mínimo TQ1
    "OPCServer1.MI2", // SP Nível Máximo TQ1

    "OPCServer1.MB2", // Status Válvula Floculador
    "OPCServer1.MI3", // Nível Real Floculador
    "OPCServer1.MI4", // SP Nível Mínimo Floculador
    "OPCServer1.MI5", // SP Nível Máximo Floculador

    "OPCServer1.MB3", // Status Válvula Filtro
    "OPCServer1.MI6", //Nível Real TQ2
    "OPCServer1.MI7", // SP Nível Máximo TQ2
    "OPCServer1.MI8", // SP Nível Mínimo TQ2
    "OPCServer1.MB4", //Status Válvula TQ2,

    "OPCServer1.MI9", //Nível Real TQ3
    "OPCServer1.MI10", // SP Nível Mínimo TQ3
    "OPCServer1.MI11", // SP Nível Máximo TQ3
    "OPCServer1.MB5", //Status Válvula TQ3

    "OPCServer1.MI12", //Nível Real TQ4
    "OPCServer1.MI13", // SP Nível Mínimo TQ4
    "OPCServer1.MI14", // SP Nível Máximo TQ4

    "OPCServer1.MB6", //Status Válvula Sulfato
    "OPCServer1.MI21", // Nível Real Sulfato Alum.
    "OPCServer1.MI22", // Nível Máx. Sulfato

    "OPCServer1.MB7", //Status Válvula Soda
    "OPCServer1.MI24", // Nível Real Soda
    "OPCServer1.MI25", // Nível Máx. Soda

    "OPCServer1.MB8", //Status Válvula Cloro
    "OPCServer1.MI27", // Nível Real Cloro
    "OPCServer1.MI28", // Nível Máx. Cloro

    "OPCServer1.MB9", //Status Válvula Cloro
    "OPCServer1.MI31", // Nível Real Cloro
    "OPCServer1.MI32", // Nível Máx. Cloro

    "OPCServer1.MB10", //Status Válvula Cloro
    "OPCServer1.MI34", // Nível Real Cloro
    "OPCServer1.MI35", // Nível Máx. Cloro

    "OPCServer1.MB11", // Status Motor TQ5
    "OPCServer1.MI101", // Consumo Água

```

```

        "OPCServer1.MB101" //Status de Comunicação com o PLC
    };

    Opc.Da.Item[] opcltems = new Item[aryItems.Length];
    int iltemIx = 0;

    foreach (string sltem in aryItems)
    {
        Opc.Da.Item opcltemCalib = new Item();
        opcltemCalib.ItemName = sltem;
        opcltems[iltemIx] = opcltemCalib;

        iltemIx++;
    }

    opcltems = opcSubscription.AddItems(opcltems);

    opcSubscription.DataChanged += new
    DataChangedEventHandler(opcSubscription_DataChanged);
    }
    catch (Exception errMsg)
    {
        MessageBox.Show(errMsg.Message.ToString(), "SABESP",
        MessageBoxButtons.OK, MessageBoxIcon.Error);
    }
}

void opcSubscription_DataChanged(object subscriptionHandle, object
requestHandle, ItemValueResult[] values)
{
    try
    {
        foreach (ItemValueResult SensorValue in values)
        {
            switch (SensorValue.ItemName)
            {
                case "OPCServer1.MB0":
                    sTQ1StatusMotor = SensorValue.Value.ToString();
                    break;

                case "OPCServer1.MI0":
                    sTQ1NivelReal = SensorValue.Value.ToString();
                    break;

                case "OPCServer1.MI1":
                    sTQ1NivelMin = SensorValue.Value.ToString();
                    break;

                case "OPCServer1.MI2":
                    sTQ1NivelMax = SensorValue.Value.ToString();

```

```
break;

case "OPCServer1.MB2":
    sFLStatusValvula = SensorValue.Value.ToString();
    break;

case "OPCServer1.MI3":
    sFLNivelReal = SensorValue.Value.ToString();
    break;

case "OPCServer1.MI4":
    sFLNivelMin = SensorValue.Value.ToString();
    break;

case "OPCServer1.MI5":
    sFLNivelMax = SensorValue.Value.ToString();
    break;

case "OPCServer1.MB3":
    sFILStatusValvula = SensorValue.Value.ToString();
    break;

case "OPCServer1.MI6":
    sTQ2NivelReal = SensorValue.Value.ToString();
    break;

case "OPCServer1.MI7":
    sTQ2NivelMax = SensorValue.Value.ToString();
    break;

case "OPCServer1.MI8":
    sTQ2NivelMin = SensorValue.Value.ToString();
    break;

case "OPCServer1.MB4":
    sTQ2StatusValvula = SensorValue.Value.ToString();
    break;

case "OPCServer1.MI9":
    sTQ3NivelReal = SensorValue.Value.ToString();
    break;

case "OPCServer1.MI10":
    sTQ3NivelMax = SensorValue.Value.ToString();
    break;

case "OPCServer1.MI11":
    sTQ3NivelMin = SensorValue.Value.ToString();
```

```

        break;

    case "OPCServer1.MB5":
        sTQ3StatusValvula = SensorValue.Value.ToString();
        break;

    //Tanque 4
    case "OPCServer1.MI12":
        sTQ4NivelReal = SensorValue.Value.ToString();
        break;
    case "OPCServer1.MI13":
        sTQ4NivelMin = SensorValue.Value.ToString();
        break;
    case "OPCServer1.MI14":
        sTQ4NivelMax = SensorValue.Value.ToString();
        break;

    //Dos. Sulfato
    case "OPCServer1.MI21":
        sSFReal = SensorValue.Value.ToString();
        break;
    case "OPCServer1.MI22":
        sSFSetPoint = SensorValue.Value.ToString();
        break;
    case "OPCServer1.MB6":
        sSFStatusValvula = SensorValue.Value.ToString();
        break;

    //Dos. Soda
    case "OPCServer1.MI24":
        sSDReal = SensorValue.Value.ToString();
        break;
    case "OPCServer1.MI25":
        sSDSetPoint = SensorValue.Value.ToString();
        break;
    case "OPCServer1.MB7":
        sSDStatusValvula = SensorValue.Value.ToString();
        break;

    //Dos. Cloro TQ1
    case "OPCServer1.MI27":
        sCLReal = SensorValue.Value.ToString();
        break;
    case "OPCServer1.MI28":
        sCLSetPoint = SensorValue.Value.ToString();
        break;
    case "OPCServer1.MB8":
        sCLStatusValvula = SensorValue.Value.ToString();
        break;

```

```

//Dos. Cloro TQ3
case "OPCServer1.MI31":
    sCLTQ3Real = SensorValue.Value.ToString();
    break;
case "OPCServer1.MI32":
    sCLTQ3SetPoint = SensorValue.Value.ToString();
    break;
case "OPCServer1.MB9":
    sCLTQ3StatusValvula = SensorValue.Value.ToString();
    break;

//Dos. Fluor TQ3
case "OPCServer1.MI34":
    sFLTQ3Real = SensorValue.Value.ToString();
    break;
case "OPCServer1.MI35":
    sFLTQ3SetPoint = SensorValue.Value.ToString();
    break;
case "OPCServer1.MB10":
    sFLTQ3StatusValvula = SensorValue.Value.ToString();
    break;

//Tanque TQ5
case "OPCServer1.MB11":
    sTQ5StatusMotor = SensorValue.Value.ToString();
    break;

//Consumo de Água
case "OPCServer1.MI101":
    sConsumoAgua = SensorValue.Value.ToString();
    break;

//Status do Processo
case "OPCServer1.MI100":
    sStatusProcesso = SensorValue.Value.ToString();
    break;

//Status de Comunicação com o PLC
case "OPCServer1.MB101":
    sStatusPLC = SensorValue.Value.ToString();
    break;
    }
}
}
catch (Exception errMsg)
{
    //Log
    //Utils.SaveLog("", "Aplicativo", errMsg.Message, 0);
}
}

```



```

private void frmSimulador_Load(object sender, EventArgs e)
{
    try
    {
        OpcCollector = Utils.GetPSOpcCollector("localhost");
        OpcServer = Utils.GetOPCServer(OpcCollector.Hostname);

        //Get all tags
        PsTag[] SAEPSTags = Utils.GetTag();

        //Create tags hashtable
        SAETags = new Hashtable();

        foreach (PsTag oTag in SAEPSTags)
            SAETags.Add(oTag.ItemName, oTag);

        LoadOPCSettings();
    }
    catch (Exception err)
    {
        MessageBox.Show(err.Message.ToString(), "SABESP",
        MessageBoxButtons.OK, MessageBoxIcon.Error);
    }
}

//Timer do Status do Motor Coleta de Água
private void tmrPump1_Tick(object sender, EventArgs e)
{
    try
    {
        pctMotor1.Image = imgListPump1.Images[iPumpIndex];
        iPumpIndex++;
        if (iPumpIndex == 4) iPumpIndex = 0;
    }
    catch { }
}

private void tmrDadosIniciais_Tick(object sender, EventArgs e)
{
    tmrDadosIniciais.Enabled = false;

    try
    {
        //Nível Real TQ 1
        lblNivelTQ1.Text = sTQ1NivelReal + " l";
        lblSPMinTQ.Text = "SetPoint Min.:" + sTQ1NivelMin + " l";
        lblSPMaxTQ.Text = "SetPoint Max.:" + sTQ1NivelMax + " l";

        //Válvula Flocculador
    }
}

```

```

        lblNivelFloc.Text = sFLNivelReal + " l";
        pctFLValvula.Image = sFLStatusValvula == "True" ? imgVert.Images[1] :
imgVert.Images[0];

```

```

        //Válvula Filtro
        pctFILValvula.Image = sFILStatusValvula == "True" ? imgVert.Images[1] :
imgVert.Images[0];
        pctStatusMotor.Image = sFILStatusValvula == "True" ?
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\BallGreen.gif") :
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\BallRed.gif");

```

```

        //Valvula TQ2
        lblNivelTQ2.Text = sTQ2NivelReal + " l";
        lblTQ2SPMin.Text = "Min.:" + sTQ2NivelMin + " l";
        lblTQ2SPMax.Text = "Max.:" + sTQ2NivelMax + " l";

```

```

        //Válvula Mistura TQ2
        pctTQ2Valv.Image = sTQ2StatusValvula == "True" ? imgVert.Images[1] :
imgVert.Images[0];

```

```

        //Valvula TQ3
        lblNivelTQ3.Text = sTQ3NivelReal + " l";
        lblTQ3SPMin.Text = "Min.:" + sTQ3NivelMin + " l";
        lblTQ3SPMax.Text = "Max.:" + sTQ3NivelMax + " l";

```

```

        //Válvula Mistura TQ3
        pctTQ3Valv.Image = sTQ3StatusValvula == "True" ? imgVert.Images[1] :
imgVert.Images[0];

```

```

        //Valvula TQ4
        lblNivelTQ4.Text = sTQ4NivelReal + " l";
        lblTQ4SPMin.Text = "Min.:" + sTQ4NivelMin + " l";
        lblTQ4SPMax.Text = "Max.:" + sTQ4NivelMax + " l";

```

```

        //Válvula Tanque Distribuição
        pctTQ5Valvula.Image = sTQ5StatusMotor == "True" ? imgVert.Images[1] :
imgVert.Images[0];

```

```

        //Dosagem Sulfato
        pctValvulaSulfato.Image = sSFStatusValvula == "True" ?
imgListValvule.Images[1] : imgListValvule.Images[0];
        lblSFReal.Text = sSFReal + " %";
        lblSFSetPoint.Text = "SetPoint: " + sSFSetPoint + " %";

```

```

        //Dosagem Soda
        pctValvulaSoda.Image = sSDStatusValvula == "True" ?
imgListValvule.Images[1] : imgListValvule.Images[0];
        lblSDReal.Text = sSDReal + " %";
        lblSDSetPoint.Text = "SetPoint: " + sSDSetPoint + " %";

```

```

//Dosagem Cloro TQ1
lblCLSetPoint.Text = "SetPoint: " + sCLSetPoint + " %";

if (sCLStatusValvula == "True")
{
    pctValvulaCloroTQ1.Image = sCLStatusValvula == "True" ?
imgVert.Images[1] : imgVert.Images[0];
    lblCLReal.Text = sCLReal + " %";
}

if (sCLTQ3StatusValvula == "True")
{
    pctValvulaCloroTQ3.Image = sCLTQ3StatusValvula == "True" ?
imgVert.Images[1] : imgVert.Images[0];
    lblCLReal.Text = sCLTQ3Real + " %";
}

if (sCLStatusValvula == "False" && sCLTQ3StatusValvula == "False")
{
    pctValvulaCloroTQ1.Image = sCLStatusValvula == "True" ?
imgVert.Images[1] : imgVert.Images[0];
    pctValvulaCloroTQ3.Image = sCLTQ3StatusValvula == "True" ?
imgVert.Images[1] : imgVert.Images[0];

    lblCLReal.Text = sCLTQ3Real + " %";
}

//Dosagem Fluor
pctValvulaFluor.Image = sFLTQ3StatusValvula == "True" ?
imgVert.Images[1] : imgVert.Images[0];
lblFLReal.Text = sFLTQ3Real + " %";
lblFLSetPoint.Text = "SetPoint: " + sFLTQ3SetPoint + " %";

lblConsumo.Text = sConsumoAgua + " l";

//Motor 1
if (sTQ1StatusMotor == "True" && tmrPump1.Enabled == false)
{
    tmrPump1.Enabled = true;
}
else if (sTQ1StatusMotor == "False" && tmrPump1.Enabled == true)
{
    tmrPump1.Enabled = false;
    pctMotor1.Image = imgPumpStop.Images[0];
}
}
finally
{
    tmrDadosIniciais.Enabled = true;
}

```

```

    }

    private void pictureBox2_Click(object sender, EventArgs e)
    {
        string sDosagem = Microsoft.VisualBasic.Interaction.InputBox("Quantidade a
ser dosada!", "ETA", string.Empty, 100, 100);

        try
        {
            if (sDosagem != "")
            {
                //Quantidade de Sulfato de Alumínio a ser dosada
                Utils.WriteOPCItem(new string[] { "OPCServer1.MI10" }, new string[] {
sDosagem });
            }
        }
        finally { }
    }

    private void pctSoda_Click(object sender, EventArgs e)
    {
        string sDosagem = Microsoft.VisualBasic.Interaction.InputBox("Quantidade a
ser dosada!", "ETA", string.Empty, 100, 100);

        try
        {
            if (sDosagem != "")
            {
                //Quantidade de Soda a ser dosada
                Utils.WriteOPCItem(new string[] { "OPCServer1.MI11" }, new string[] {
sDosagem });
            }
        }
        finally { }
    }

    private void pictureBox5_Click(object sender, EventArgs e)
    {
        string sDosagem = Microsoft.VisualBasic.Interaction.InputBox("Quantidade a
ser dosada!", "ETA", string.Empty, 100, 100);

        try
        {
            if (sDosagem != "")
            {
                //Quantidade de Cloro a ser dosada
                Utils.WriteOPCItem(new string[] { "IOP.static.I1" }, new string[] {
sDosagem });
            }
        }
    }

```

```

    }

    }
    finally {}
}

private void pictureBox7_Click(object sender, EventArgs e)
{
    string sDosagem = Microsoft.VisualBasic.Interaction.InputBox("Quantidade a
ser dosada!", "ETA", string.Empty, 100, 100);

    try
    {
        if (sDosagem != "")
        {
            //Quantidade de Fluor a ser dosada
            Utils.WriteOPCItem(new string[] { "IOP.static.I1" }, new string[] {
sDosagem });
        }
    }
    finally {}
}

// Trabalha com o Nível dos Tanques
private void tmrDesceNivel_Tick(object sender, EventArgs e)
{
    try
    {
        iTQ1Nivel = int.Parse(sTQ1NivelReal);

        if (iTQ1Nivel < 1000)
        {
            //pctNivelAgua10.Image
            Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\NivelAgua10.png");
            pctAgua1.Visible = false;
            pctAgua2.Visible = false;
            pctAgua3.Visible = false;
            pctAgua4.Visible = false;
            pctAgua5.Visible = false;
            pctAgua6.Visible = false;

            if (!pctTQ1SensorMin.Visible)
            {
                pctTQ1SensorMin.Visible = true;
                pctTQ1SensorMax.Visible = false;
            }
        }
    }
}

```

```

else if (iTQ1Nivel > 1000 && iTQ1Nivel < 5000)
{
    //pctNivelAgua10.Image
    Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\NivelAgua9.png");
    pctAgua1.Visible = true;
    pctAgua2.Visible = false;
    pctAgua3.Visible = false;
    pctAgua4.Visible = false;
    pctAgua5.Visible = false;
    pctAgua6.Visible = false;

    if (pctTQ1SensorMin.Visible)
    {
        pctTQ1SensorMin.Visible = false;
        pctTQ1SensorMax.Visible = false;
    }
}

else if (iTQ1Nivel > 5000 && iTQ1Nivel < 10000)
{
    //pctNivelAgua10.Image
    Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\NivelAgua8.png");
    pctAgua1.Visible = true;
    pctAgua2.Visible = true;
    pctAgua3.Visible = false;
    pctAgua4.Visible = false;
    pctAgua5.Visible = false;
    pctAgua6.Visible = false;
}

else if (iTQ1Nivel > 10000 && iTQ1Nivel < 15000)
{
    //pctNivelAgua10.Image
    Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\NivelAgua7.png");
    pctAgua1.Visible = true;
    pctAgua2.Visible = true;
    pctAgua3.Visible = true;
    pctAgua4.Visible = false;
    pctAgua5.Visible = false;
    pctAgua6.Visible = false;
}

else if (iTQ1Nivel > 15000 && iTQ1Nivel < 20000)
{
    //pctNivelAgua10.Image
    Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\NivelAgua6.png");
    pctAgua1.Visible = true;
    pctAgua2.Visible = true;
    pctAgua3.Visible = true;
    pctAgua4.Visible = true;
    pctAgua5.Visible = false;

```

```

        pctAgua6.Visible = false;
    }

    else if (iTQ1Nivel > 20000 && iTQ1Nivel < 25000)
    {
        //pctNivelAgua10.Image
        Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\NivelAgua5.png");
        pctAgua1.Visible = true;
        pctAgua2.Visible = true;
        pctAgua3.Visible = true;
        pctAgua4.Visible = true;
        pctAgua5.Visible = true;
        pctAgua6.Visible = false;
    }
    //else if (iTQ1Nivel > 15000 && iTQ1Nivel < 18000)
    //
    //                                pctNivelAgua10.Image
    Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\NivelAgua4.png");

    //else if (iTQ1Nivel > 18000 && iTQ1Nivel < 21000)
    //
    //                                pctNivelAgua10.Image
    Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\NivelAgua3.png");
    //else if (iTQ1Nivel > 21000 && iTQ1Nivel < 24000)
    //
    //                                pctNivelAgua10.Image
    Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\NivelAgua2.png");
    else if (iTQ1Nivel > 25000)
    {
        //pctNivelAgua10.Image
        Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\NivelAgua1.png");
        pctAgua1.Visible = true;
        pctAgua2.Visible = true;
        pctAgua3.Visible = true;
        pctAgua4.Visible = true;
        pctAgua5.Visible = true;
        pctAgua6.Visible = true;
    }

    if (iTQ1Nivel > 28000)
    {
        if (pctTQ1SensorMax.Visible)
        {
            pctTQ1SensorMax.Visible = true;
            pctTQ1SensorMin.Visible = false;
        }
    }
}
catch
{
}
}

```

```

private void btnStopProcess_Click(object sender, EventArgs e)
{
    try
    {
        if (sStatusProcesso == "True")
        {
            MessageBox.Show("PROCESSO JÁ ESTÁ PARADO!", "SABESP",
                MessageBoxButtons.OK, MessageBoxIcon.Information);
            return;
        }

        if (MessageBox.Show("DESEJA PARAR O PROCESSO ?", "SABESP",
            MessageBoxButtons.YesNo, MessageBoxIcon.Question) == DialogResult.Yes)
        {
            //Parar o Processo
            Utils.WriteOPCItem(new string[] { "OPCServer1.MB100" }, new string[] {
"0" });
        }

    }
    catch (Exception err)
    {
        MessageBox.Show(err.Message.ToString(), "SABESP",
            MessageBoxButtons.OK, MessageBoxIcon.Error);
    }
    finally { }
}

private void btnStartProcess_Click(object sender, EventArgs e)
{
    try
    {
        if (sStatusProcesso == "True")
        {
            MessageBox.Show("PROCESSO JÁ INICIADO!", "SABESP",
                MessageBoxButtons.OK, MessageBoxIcon.Information);
            return;
        }

        if (MessageBox.Show("DESEJA INICIAR O PROCESSO ?", "SABESP",
            MessageBoxButtons.YesNo, MessageBoxIcon.Question) == DialogResult.Yes)
        {
            //Zera as Variáveis
            Utils.WriteOPCItem(new string[] { "OPCServer1.MI0" }, new string[] { "0" });
            Utils.WriteOPCItem(new string[] { "OPCServer1.MI3" }, new string[] { "0" });
            Utils.WriteOPCItem(new string[] { "OPCServer1.MI6" }, new string[] { "0" });
            Utils.WriteOPCItem(new string[] { "OPCServer1.MI9" }, new string[] { "0" });
            Utils.WriteOPCItem(new string[] { "OPCServer1.MI12" }, new string[] { "0"
});
        }
    }
}

```



```

        //Inicia o Processo
        Utils.WriteOPCItem(new string[] { "OPCServer1.MB100" }, new string[] {
"1" });
    }

    }
    catch (Exception err)
    {
        MessageBox.Show(err.Message.ToString(), "SABESP",
        MessageBoxButtons.OK, MessageBoxIcon.Error);
    }
    finally { }
}

private void tmrHelice_Tick(object sender, EventArgs e)
{
    try
    {
        if (sFLStatusValvula == "True")
        {
            if (iHelice == 0)
            {
                pc1.Visible = true;
                pc2.Visible = false;
            }
            else if (iHelice == 1)
            {
                pc1.Visible = false;
                pc2.Visible = true;
            }
        }
        else
        {
            pc1.Visible = true;
            pc2.Visible = false;
        }
    }

    iHelice++;
    if (iHelice == 2) iHelice = 0;
}
catch { }
}

private void tmrStatusPLC_Tick(object sender, EventArgs e)
{
    try
    {
        if (sStatusPLC == "True")
        {

```

```

        pctLiga3.Image =
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Ligado.png");
        pctLiga4.Image =
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Ligado.png");
        pctLiga5.Image =
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Ligado.png");
        pctLiga6.Image =
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Ligado.png");
        pctLiga7.Image =
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Ligado.png");
        pctLiga8.Image =
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Ligado.png");
    }
    else
    {
        pctLiga3.Image =
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Desligado.png");
        pctLiga4.Image =
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Desligado.png");
        pctLiga5.Image =
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Desligado.png");
        pctLiga6.Image =
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Desligado.png");
        pctLiga7.Image =
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Desligado.png");
        pctLiga8.Image =
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Desligado.png");
    }
}
catch { }
}

private void tmrComunicacaoRede_Tick(object sender, EventArgs e)
{
    try
    {
        if (sStatusPLC == "True")
        {
            if (iStatusComunicacao == 0)
            {
                pctLiga1.Image =
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Ligado.png");
                pctLiga2.Image =
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Ligado.png");
            }
            else if (iStatusComunicacao == 1)
            {
                pctLiga1.Image =
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Comunica.png");
            }
        }
    }
}

```

```

        pctLiga2.Image
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Comunica.png");
    }
    }
    else
    {
        pctLiga1.Image
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Desligado.png");
        pctLiga2.Image
Image.FromFile(@"C:\Projetos\SumAguaEsgoto\Imagens\Desligado.png");
    }

    iStatusComunicacao++;
    if (iStatusComunicacao == 2) iStatusComunicacao = 0;
}
catch {}
}
}

```