CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

Mauro Henrique Sardinha

SEGURANÇA E AUTOMAÇÃO DE SISTEMAS DE TRATAMENTO DE ÁGUA

Americana, SP
2015

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Mauro Henrique Sardinha

SEGURANÇA E AUTOMAÇÃO DE SISTEMAS DE TRATAMENTO DE ÁGUA

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Professor Esp. Carlos Frederico Faé.

Área de concentração: Redes de Computadores.

Americana, SP

2015

Sardinha, Mauro Henrique
S Segurança e automação de sistemas de
249s tratamento de água. / Mauro Henrique Sardinha. – Americana: 2015.
67f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Esp. Carlos Frederico Faé

1. Automação industrial 2. Proteção ao meio ambiente 3. Sistemas de informação I. Faé, Carlos Frederico II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 658.52.56
504.06
681.518

Mauro Henrique Sardinha

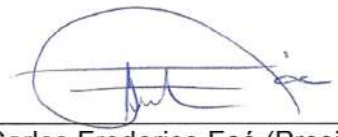
SEGURANÇA E AUTOMAÇÃO DE SISTEMAS DE TRATAMENTO DE ÁGUA

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Redes de Computadores.

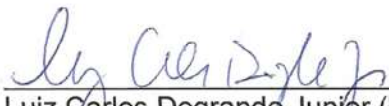
Americana, 23 de Junho de 2015.

Banca Examinadora:



Carlos Frederico Faé (Presidente)
Especialista
Fatec - Americana

Benedito Aparecido Cruz (Membro)
Especialista
Fatec – Americana



Luiz Carlos Degrande Junior (Membro)
Graduado
Fatec - Americana

AGRADECIMENTOS

Em primeiro lugar, a Deus que me proporcionou a oportunidade de estudo e preparou o caminho para o conhecimento.

Aos colegas da Fatec que me auxiliaram na busca pelos objetivos, em especial ao Arthur, Carlos Eduardo, Marcelo e Matheus.

Aos professores da Fatec, em especial, meu Orientador: Prof. Esp. Carlos Frederico Faé, que por muitas vezes guiou-me sabiamente no caminho assertivo do desenvolvimento do estudo.

À minha namorada Janaína de Oliveira Santoandréa pela paciência e compreensão.

Ao DAE de Santa Bárbara, que me proporcionou a oportunidade do aprendizado.

DEDICATÓRIA

É com grande orgulho que dedico a confecção deste projeto à minha namorada, mãe, pai, irmãos e ao meu orientador, Prof. Esp. Carlos Frederico Faé, que contribuíram de forma singular para minha jornada de estudo.

RESUMO

Introduzindo conceitos sobre os assuntos Tratamento de Água, Automação, Redes de Computadores e Segurança da Informação, este trabalho tem o objetivo de mostrar a utilização da automação como fonte de segurança das informações de um sistema convencional de tratamento de água. Após apresentar ao leitor as etapas e as variáveis de um sistema de tratamento de água convencional, traz a explanação de um sistema de automação voltado para a operação de tratamento, utilizando equipamentos de medição inteligentes com tecnologia embarcada. Expõe ainda as redes de campo com o protocolo RS485 como forma de conectar estes instrumentos à um CLP, que faz toda a comunicação com o software de controle da estação já automatizada. Em seguida aborda a concepção de uma Política de Segurança da Informação como forma de proteção tanto dos equipamentos instalados como das informações geradas por este sistema. Utilizando-se da metodologia de estudo de caso, o projeto indica os resultados do investimento em saneamento básico como forma de economia de recursos, além da gestão e segurança da informação, comprovando o objetivo do trabalho.

Palavras Chave: Segurança da Informação; Redes; Automação; Tratamento de Água.

ABSTRACT

Introducing concepts of Water Treatment, Automation, Computer Networks and Information Security, this project aims to show the use of automation as a source of security information of a conventional water treatment system. After introducing the reader to the steps and variables of a conventional water treatment system, brings the explanation of an automation system designed for the treatment operation using smart metering equipment with embedded technology. Also exposes the field networks with RS485 protocol as a way to connect these instruments to a PLC, which makes all communication with the control software in station already automated. Next it discusses the creation of an Information Security Policy to protect both the equipment installed as the information generated by this system. Using the case study methodology, the project indicates the results of investment in sanitation as a means of saving resources, as well as management and information security, proving the purpose of the work.

Keywords*: Information Security; Networks; Automation; Water Treatment.*

SUMÁRIO

LISTA DE FIGURAS

1. INTRODUÇÃO

Desde os primórdios da humanidade, o homem convive com a informação da mesma forma que convive com a energia. Porém, ainda não foi possível elaborar um conceito que seja aceitável de forma científica como foi o de $E=mc^2$, para energia. As definições disponíveis nos dicionários são ricas em argumentos circulares que talvez até consigam nos descrever o que é a informação de fato. Ferreira (1996, p. 944), conhecido dicionário da língua portuguesa, apresenta informação como “ato ou efeito de informar (se); informe; dados a respeito de alguém; conhecimento, participação; instrução.”. A exata noção sobre informação é bem vaga e intuitiva, e ela pode ser usada, assimilada, manipulada, transformada, produzida e transmitida no tempo e no espaço de diversas maneiras. Em síntese, definir com exatidão o conceito informação é um desafio.

Em contrapartida ao termo informação exposto anteriormente, a palavra segurança apresenta grande diversidade em seu significado, sendo objeto dos mais variados estudos. Em dicionário da Língua Portuguesa, a palavra segurança é definida com os seguintes significados:

> 1) Ato ou efeito de segurar; 2) Estado, qualidade ou condição de seguro; 3) Condição daquele ou daquilo em que se pode confiar; 4) Certeza, firmeza, convicção; 5) Confiança em si mesmo, autoconfiança; 6) Caução, garantia, seguro; 7) Protesto, afirmação; 8) Prenhez das fêmeas dos quadrúpedes; 9) Pessoa encarregada da segurança pessoal de alguém ou de empresa, guardacosta. (FERREIRA, 1996, p. 1563)

De forma específica, a segunda definição – estado, qualidade ou condição de seguro – para o termo segurança nos apresenta um valor extraordinário, sendo referendada em muitas outras fontes de pesquisa. Segurança é “um estado, qualidade ou condição de uma pessoa ou coisa que está livre de perigos, de incertezas, assegurada de danos e riscos eventuais, afastada de todo mal” (Houaiss).

A norma ISO/IEC (Organização Internacional para Padronização) 27002 da ABNT (Associação Brasileira de Normas Técnicas) (2005 p. X) define a SI (Segurança da Informação) como: “a proteção da informação de vários tipos de

ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre investimentos e as oportunidades de negócio".

A concepção de segurança adotada pela ISO/IEC 27002 pode ser entendida como um ato de proteção para defender a informação que está em um ambiente de perigo, risco ou incerteza. Para obter segurança é necessária a implementação de controles que devem ser selecionados e utilizados para assegurar que os riscos sejam reduzidos a um nível aceitável pela organização.

A segurança de uma determinada informação pode ser afetada por fatores comportamentais e do uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação e tem como principais atributos: Confidencialidade, Integridade e Disponibilidade.

Cerca de 70% da superfície da Terra está coberta por água. Deste total, aproximadamente 97% é água salgada e está nos oceanos. Apenas cerca de 3% de toda a água do planeta é doce, onde 2% estão nas geleiras, e apenas cerca de 1% está disponível em corpos d'água da superfície, isto é, rios, lagos, e sendo que a maior parte, ou seja, 95% encontram-se no subsolo.

Para que possamos utilizar dessa água em nosso cotidiano, é necessário que a mesma passe por um processo de tratamento, garantindo que a água torne-se potável. De acordo com a Norma Brasileira 12216 da ABNT uma Estação de Tratamento de Água (ETA) "é o conjunto de unidades destinado a adequar as características da água bruta, isto é, como ela é encontrada no curso d'água aos padrões de potabilidade". As ETAs (Estações de Tratamento de Água) são projetadas para remoção de riscos presentes em águas captadas, por meio de uma combinação de controles, processos e de operações de tratamento. No Brasil, a qualidade da água para consumo humano é especificada atualmente pela Portaria 2.914 do Ministério da Saúde, publicada em 12 de dezembro de 2011.

Segundo Botero (2009):

> O processo convencional de tratamento de água emprega a sedimentação com uso de coagulantes e é compreendido pelas seguintes operações unitárias: coagulação, floculação, decantação, e filtração para a clarificação da água, seguida da correção do pH, desinfecção e fluoretação.

Estes processos exigem um rígido controle de dosagem de produtos químicos e um minucioso acompanhamento dos padrões de qualidade e potabilidade, e serão detalhadas posteriormente. Diversas variáveis influenciam diretamente no tratamento da água bruta e algumas das principais são: vazão, turbidez, cor, coagulante e pH (Potencial Hidrogeniônico) e também serão destrinchadas ao longo do trabalho.

Apenas para enfatizar:

> Para realizar o tratamento completo da água, a mesma deve passar por diversos procedimentos nos quais eventuais falhas podem ocorrer, resultando em custos operacionais. Assim, o tratamento de água é dividido nas seguintes etapas: Antes do tratamento: comprometimento dos mananciais, necessidade de busca de mananciais mais distantes exigindo maior consumo de energia, infraestrutura para adução, bombeamento, entre outros; Durante o tratamento: consumo de produtos químicos, controle operacional, perda de água, consumo de energia elétrica e geração de resíduos; Após o tratamento: qualidade da água tratada, análise de resíduos gerados e seu destino final. O controle de qualidade em cada etapa possibilita à estação de tratamento de água atender à critérios de qualidade e legislações pertinentes. (ACHON, 2008).

Como a maioria das ETAs possuem controles manuais de dosagem de produtos químicos, análises físico-químicas, lavagem de filtros e decantadores, e todos os outros controles operacionais dependendo totalmente da mão humana, qualquer mínimo erro de operação pode comprometer todo o sistema de tratamento, gerando diversos custos extras como, por exemplo: desperdício de produtos químicos, aumento do consumo de energia elétrica, perda de água (tanto dentro da própria ETA quanto em descargas de rede que seriam desnecessárias), maior consumo de combustíveis e insumos, enfim, diversas manutenções e despesas extras secundárias causadas por erros operacionais.

Porém, a principal preocupação é certamente quanto à qualidade da água tratada que é distribuída à população, que pode ser totalmente comprometida por um simples erro operacional, arriscando a saúde e bem estar dos consumidores e acarretando diversos outros prejuízos.

O objetivo geral deste trabalho é aplicar a automação como fonte de segurança das informações no sistema de tratamento de água da autarquia municipal de Santa Bárbara d'Oeste.

Como objetivos específicos, este trabalho apresenta melhoria no processo de tratamento de água, tornando-a mais segura para o consumo humano em geral, e com o investimento trazer economia e eficiência à autarquia, cumprindo também com o artigo 13°, Inciso X da portaria 2.914/11 do MS, a saber:

> proporcionar mecanismos para recebimento de reclamações e manter registros atualizados sobre a qualidade da água distribuída, sistematizando-os de forma compreensível aos consumidores e disponibilizando-os para pronto acesso e consulta pública, em atendimento às legislações específicas de defesa do consumidor;

O método científico de pesquisa utilizado foi o de procedimentos com a modalidade de estudo de caso, podendo ser classificado em relação à sua natureza como pesquisa aplicada. Quanto aos procedimentos técnicos utilizados, destacam-se o bibliográfico e o documental, visto que a maioria do material utilizado nesta pesquisa provém de arquivos e matérias obtidos em sala de aula, com os próprios professores da Fatec.

O trabalho está estruturado em 8 capítulos, sendo que o primeiro contém uma introdução aos assuntos a serem abordados, o problema central, os objetivos e a metodologia científica de pesquisa. Já o segundo capítulo traz uma revisão de bibliografia, e a partir do terceiro capítulo o trabalho mostra uma série de explanações, iniciando com a caracterização da empresa estudada e o processo de tratamento de água. No quarto capítulo, há uma exposição sobre automação e instrumentos de medição com tecnologia embarcada. O quinto capítulo faz uma básica explanação sobre redes de computadores, sendo complementado pelo sexto capítulo que exibe conceitos essenciais de segurança da informação. O sétimo capítulo expõe a aplicação dos conceitos para a elaboração do projeto, e no oitavo capítulo as considerações finais são apresentadas.

2. REVISÃO BIBLIOGRÁFICA

Este capítulo apresenta uma revisão bibliográfica sobre os conceitos de segurança, informação, segurança da informação, redes, automação e tratamento de água.

De acordo com Cepik (2001, p. 2):

> Segurança é uma condição relativa de proteção na qual se é capaz de neutralizar ameaças discerníveis contra a existência de alguém ou de alguma coisa. Em termos organizacionais, segurança é obtida através de padrões e medidas de proteção para conjuntos definidos de informações, sistemas, instalações, comunicações, pessoal, equipamentos ou operações.

Para Veneziano (2009-2011, p. 7):

> Uma informação é um conjunto de dados que faz sentido ou possui utilidade para alguém. É necessário que ela seja precisa, completa, econômica, flexível, confiável, relevante, simples, pontual, verificável, acessível e segura.

Já Barreto (1994, p. 1) afirma que a informação sintoniza a humanidade participando da evolução e da revolução das civilizações. Como elemento organizador, atualmente a informação tem elevada importância, sendo colocada no centro das discussões sobre a sua natureza, seu conceito e os benefícios que pode trazer para a sociedade. Qualifica-se como um instrumento modificador da consciência do homem e de seu grupo. De medida de organização passa a ser a organização em si, por meio do conhecimento, que só se realiza se a informação é percebida e aceita pelos indivíduos. A informação, adequadamente abstraída, produz conhecimento, transforma aqueles assimilados anteriormente pelas pessoas e traz resultados para o respectivo desenvolvimento, assim como de toda a sociedade em que elas vivem. A informação caracteriza-se como estruturas significantes com a competência de gerar conhecimento para o indivíduo e seu grupo.

> O aumento na disponibilidade de acesso e o refinamento constante nas técnicas de fraude resultam no crescente número de incidentes de segurança. Isto obriga as organizações a se protegerem de maneira efetiva, afinal é a sua sobrevivência que está em jogo. (NAKAMURA 2007, p. 29).

Para Robredo (2003 *apud* JESUS, 2011 p. 26):

> [...] obtemos a consciência da necessidade da implementação de práticas bem definidas para obtermos a garantia de sua confidencialidade, integridade, disponibilidade e autenticidade da informação, tendo em vista que a mesma pode ser registrada (codificada) de diversas formas, duplicada e reproduzida *ad infinitum*, transmitida por diversos meios, conservada e armazenada em suportes diversos, medida e quantificada, adicionada a outras informações, organizada, processada e reorganizada segundo critérios diversos, e recuperada quando necessário, segundo regras preestabelecidas.

Segundo definido pela norma ABNT NBR ISO/IEC 27002:2005 (2005, p. x), segurança da informação "é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio". Sendo obtida a partir da "implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware".

Nakamura (2007 *apud* COSTA, 2011 p. 6) defende que "[...] as organizações devem se utilizar dos recursos possíveis a fim de garantir a segurança da informação sensível ao seu negócio.".

De acordo com Fernandes (2011, p. 44), a internet trouxe uma imensa flexibilidade e aumento na escala da comunicação entre os sistemas em virtude da distribuição em todas as partes do mundo e a condução de imensos volumes de dados a elevadas velocidades. Com isso, circula uma grande quantidade de riqueza, que desperta a cobiça de criminosos, ocasionando insegurança na rede mundial.

Fernandes (Op. Cit.) ainda aponta 6 fatores que contribuem para a insegurança dos sistemas conectados à internet. O primeiro é o baixo risco de punição de uma pessoa que explora vulnerabilidades em protocolos do *host*. O segundo é uso dos *hosts* por pessoas com pouco conhecimento em informática, tendo em vista que podem ser enganadas por um ataque que utiliza interfaces corrompidas. O terceiro é a existência de protocolos para a *internet* concebidos numa época que não se pensava em ataques de *hackers*. O quarto é o aumento da complexidade das interfaces das aplicações computacionais que tornam os protocolos de comunicação difíceis de serem analisados. O quinto é a presença de vulnerabilidades nos programas de computador que implementam as interfaces e

nos agentes de comunicação que executam protocolos na *internet*. O sexto e último é a existência de vulnerabilidades nos programas de banco de dados expostos na *web*.

O conceito de rede de computadores surgiu no início dos anos 60 do século XX, de acordo com Simon (1997), a ARPA (*Advanced Research Projects Agency*) agência de pesquisa e projetos avançados do Departamento de Defesa dos EUA iniciou um projeto de uma rede de computadores que permitisse trabalho cooperativo entre grupos mesmo que geograficamente distantes. Surgiu então a ARPANET, que em 1970 realiza o primeiro experimento com quatro universidades.

Silveira (1998 *apud* FONSECA, 2009 p. 1) descreve a automação como "[...] um conceito e um conjunto de técnicas por meio das quais se constroem sistemas ativos capazes de atuar com uma eficiência ótima pelo uso de informações recebidas do meio sobre o qual atuam".

Já de acordo com Piovesan (1993 apud SOUZA, 2006 p. 39):

> A introdução de um microprocessador no transmissor tinha o objetivo de corrigir as não-linearidades e compensar as grandezas de influência, a fim de melhorar o desempenho do instrumento, que passaria a ter uma resposta melhor à grandeza a ser medida.

De acordo com Tsutiya (2004, p. 10), uma estação de tratamento de água é o "conjunto de unidades destinado a tratar a água de modo a adequar as suas características aos padrões de potabilidade".

Para finalizar, acrescento o que diz Mascarenhas (2005, p. 3):

> O país não poderá manter um crescimento econômico sustentado, a menos que expanda o volume e melhore a qualidade dos investimentos em infra-estrutura (*sic*). Os recursos devem ser canalizados para a eliminação de gargalos de impacto imediato e, posteriormente, devem ser alocados segundo uma lógica de prioridades, exigindo para isso um bom sistema de governança que propicie tomada de decisão.

3. O TRATAMENTO DA ÁGUA

Para muitas de nossas tarefas cotidianas e bem como para muitas atividades econômicas, a água necessita passar por um processo de tratamento, garantindo sua qualidade e, todas as etapas deste tratamento devem ser devidamente monitoradas. O processo pode tornar-se mais dificultoso dependendo das características físico-químicas e biológicas do manancial de captação dessas águas, devido à presença de maior quantidade de impurezas. De acordo com Pavanelli (2001 p. 4): “as principais impurezas encontradas nas águas superficiais são: sólidos dissolvidos em forma ionizada, gases dissolvidos, compostos orgânicos dissolvidos e matéria em suspensão, tais como, microrganismos (bactérias, algas e fungos) e coloides”.

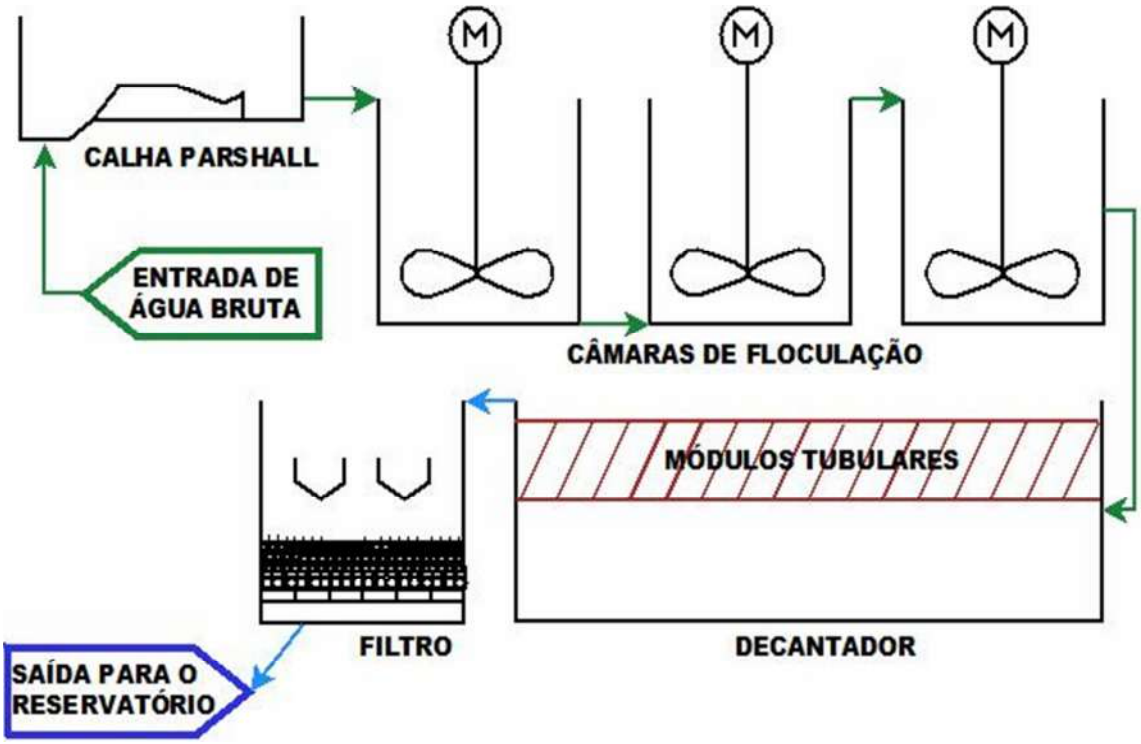
Neste capítulo, será caracterizada a empresa onde foi baseado este trabalho e em seguida a explanação do tratamento convencional com suas principais variáveis.

3.1. Caracterização da Empresa

O Departamento de Água e Esgoto (DAE) de Santa Bárbara d'Oeste é uma Autarquia Municipal criada em 1985 pela Lei Municipal nº 1649/85, cuja função é operar, manter, conservar e explorar os serviços públicos de água e esgoto do município. Como toda autarquia, é uma entidade com autonomia administrativa e personalidade jurídica, patrimônio e receita próprios. O objetivo do Departamento é tornar-se referência em serviços de água e saneamento, buscando sempre a excelência. Sua atual sede está localizada à Rua José Bonifácio, nº 400, no Centro de Santa Bárbara d’Oeste, estado de São Paulo.

Este trabalho foi realizado tomando como base as dependências da ETA IV do DAE barbarense, uma ETA do tipo convencional (coagulação/floculação, decantação e filtração) como mostra a Figura 1, localizada na Av. Prefeito Isaías Hermínio Romano, 500 - Jardim Souza Queiroz, no mesmo município. Seu manancial de captação é de origem superficial, o Ribeirão dos Toledos, através da Estação Elevatória Santa Alice.

Figura 1 - Fluxograma de uma ETA convencional - ETA IV



Fonte: Autoria Própria.

Figura 2 - Sede da Autarquia.

Fonte: Site do DAE.

3.2. Coagulação

A coagulação é um dos processos fundamentais para o tratamento de água, pois é responsável pela clarificação da água, pela remoção da maioria dos metais pesados, além de agentes químicos e microbiológicos. Macedo (2007 *apud* FRANCISCO et al [201-?] p. 4) avalia que:

> [...] a coagulação é uma das etapas mais importantes que compõe as ETAs, haja vista a necessidade de desestabilização química das partículas contidas nas águas brutas, para a posterior aglutinação e sedimentação nas unidades de floculação e decantação, respectivamente.

As impurezas presentes nas águas, que devem ser removidas ou minimizadas para fins de consumo humano, basicamente são: argilas, silicatos, íons metálicos, microrganismos (bactérias, protozoários, vírus, algas e fungos) que sobre o aspecto elétrico, em sua grande maioria apresentam carga elétrica negativa e são de tamanho minúsculo.

Para remoção destas impurezas são utilizados produtos químicos denominados de coagulante, geralmente um sal metálico de caráter ácido e solúvel em água, que fornece carga elétrica positiva e ainda que reaja com a água (hidrólise), formando complexos ou precipitados químicos.

Inúmeros são os fatores que influenciam na eficiência do processo de coagulação. Dentre eles, destacam-se: a) Dosagem do agente coagulante; b) Tempo e gradiente de velocidade de mistura rápida; c) Auxiliares de coagulação; d) pH do meio e; e) Dispersão do agente na mistura rápida.

> O pH e a dosagem do agente coagulante estão estreitamente ligados, já que cada produto químico empregado com a finalidade de promover a coagulação apresenta uma faixa ótima de pH e a simples elevação da dosagem não garante uma eficiência maior. Portanto, o devido controle dos processos envolvidos nessa etapa do tratamento, permite obter maiores eficiências com menor volume de produtos químicos (HELLER; PADUA, 2010).

Tanto a sub quanto a sobre dosagem de coagulante podem comprometer o tratamento da água, sobrecarregando as etapas subsequentes e podendo causar desconformidades com os padrões de potabilidade – Portaria: 2914/11 do Ministério da Saúde, podendo levar também ao aumento dos custos operacionais, por

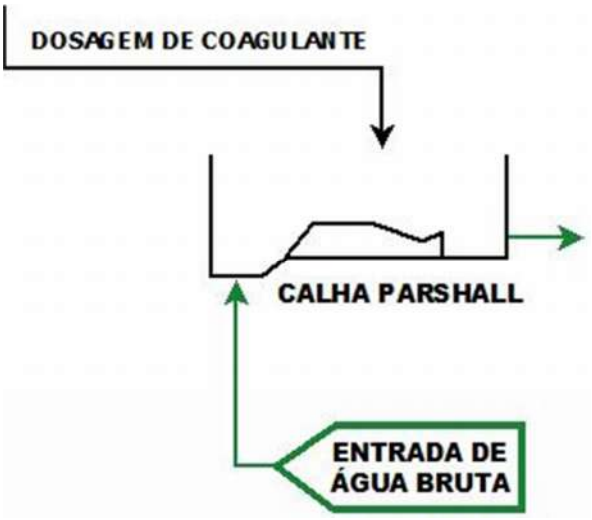
exemplo, com o aumento do consumo de água tratada utilizada para lavagem dos filtros.

Portanto, um bom controle do processo de coagulação pode reduzir custos operacionais, gastos com produtos químicos e garantir a conformidade com o Padrão de Potabilidade vigente.

De acordo com as estações do ano, qualidade do solo, tipo de manancial, entre outros, a qualidade da água bruta apresenta grande variação, podendo ser completamente diferentes em mananciais vizinhos. A dosagem de coagulante está relacionada não linearmente com os parâmetros que definem a qualidade da água bruta tais como, pH, cor, condutividade, temperatura, entre outros, e principalmente, à turbidez. Como essas relações nem sempre são conhecidas detalhadamente, a determinação da quantidade de coagulante a ser dosado é difícil de ser calculada.

Atualmente a ETA IV utiliza o PAC (Policloreto de Alumínio) com basicidade como coagulante, um produto químico de caráter ácido que se apresenta na forma líquida (entre 9% e 11% de óxidos de alumínio), dosado na Calha Parshall como mostra a Figura 3, através de bombas dosadoras controladas manualmente com acionamento por inversores de frequência. Na maioria das ETAs, assim como a ETA IV barbarense, o controle do processo de coagulação é feito de forma manual, utilizando-se de cronômetro e proveta para a checagem de dosagem do coagulante, e a posterior coleta de amostra para a verificação do pH (Potencial Hidrogeniônico) desta água coagulada.

Figura 3 - Ponto de dosagem do coagulante.



Fonte: Autoria Própria.

3.2.1. pH Ótimo de Coagulação

Cada coagulante existente possui uma faixa de pH ótimo de coagulação, que pode variar de acordo com a qualidade da água bruta. Na ETA IV, a faixa ideal encontrada, em testes previamente realizados, foi uma média entre 6,4 e 6,8.

A definição de pH (Potencial Hidrogeniônico) consiste em: **pH = -log aH^+**, onde **a** corresponde à atividade dos íons H^+ (íons de Hidrogênio) em solução aquosa. De maneira genérica, podemos dizer que o pH corresponde à concentração de íons H^+ presentes na solução a ser analisada.

A média de valores encontrados para o pH da água bruta que chega para tratamento na ETA IV é de 6,8. Com a adição do PAC para a coagulação o pH da água tende a baixar, mesmo com a basicidade apresentada pelo produto. Para que o pH ótimo de coagulação seja alcançado, faz-se necessária a dosagem de um agente alcalinizante, que neste caso, é o Hidróxido de Cálcio em Suspensão Aquosa, fornecido à esta autarquia na forma líquida (entre 19% e 21% de Hidróxido de Cálcio). A dosagem deste alcalinizante é feita por bombas de controle manual acionadas por inversores de frequência, e, de acordo com o valor de pH encontrado na amostra analisada, o operador faz a correção de dosagem, se necessário.

3.3. Floculação

A floculação é a etapa onde ocorre o agrupamento das partículas previamente desestabilizadas pela coagulação, visando à formação de flocos com tamanho e massa que favoreçam sua remoção na etapa seguinte.

No início da floculação, logo após a coagulação, as impurezas ainda encontram-se dispersas na água, sendo necessária agitação mais intensa (maior gradiente de velocidade médio) para permitir o contato entre elas, visando à agregação destas em flocos. À medida que os flocos vão se formando, o gradiente de velocidade médio deve ser reduzido, a fim de atenuar a quebra daqueles já existentes. Para isso, a água passa por mais de uma câmara de floculação, denominada também de floculador.

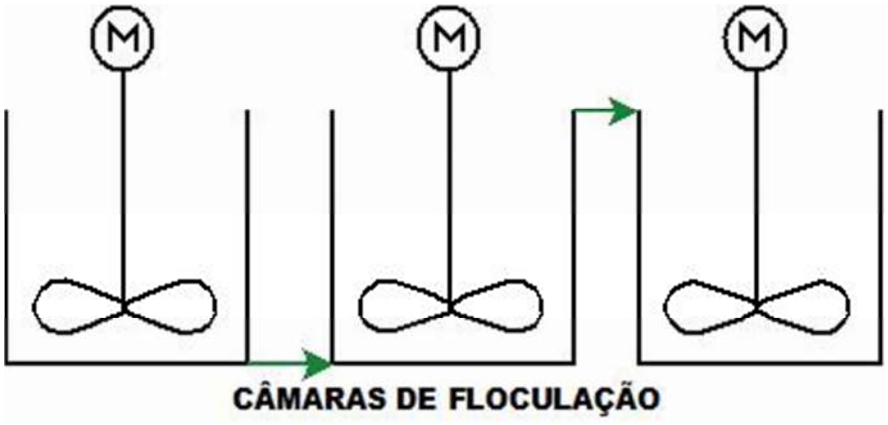
A floculação é um processo fundamentalmente físico e consiste no transporte das espécies hidrolisadas, para que haja contato com as impurezas presentes na

água, formando partículas maiores denominadas flocos. É um processo rápido e depende essencialmente do pH, da temperatura, da quantidade de impurezas. Nesta etapa há a necessidade de agitação relativamente lenta, para que ocorram choques entre as partículas.

> Nas ETAs a floculação pode ocorrer de forma hidráulica ou mecânica. Embora a floculação hidráulica apresente menor custo de construção e manutenção e maior simplicidade de operação, ela não possui a flexibilidade quanto à alteração dos valores de gradientes de velocidade média, o que pode tornar inadequada a sua aplicação em ETAs em que a água bruta apresenta, sazonalmente, grande variação de qualidade (HELLER; PADUA, 2010).

A ETA IV possui três floculadores em série como indicado na Figura 4, e com isso, três gradientes diferentes de velocidade que são ajustadas manualmente através de inversores de frequência pelo operador da estação, o que permite uma formação de flocos consistentes para a próxima etapa.

Figura 4 – Floculadores.



Fonte: Autoria Própria.

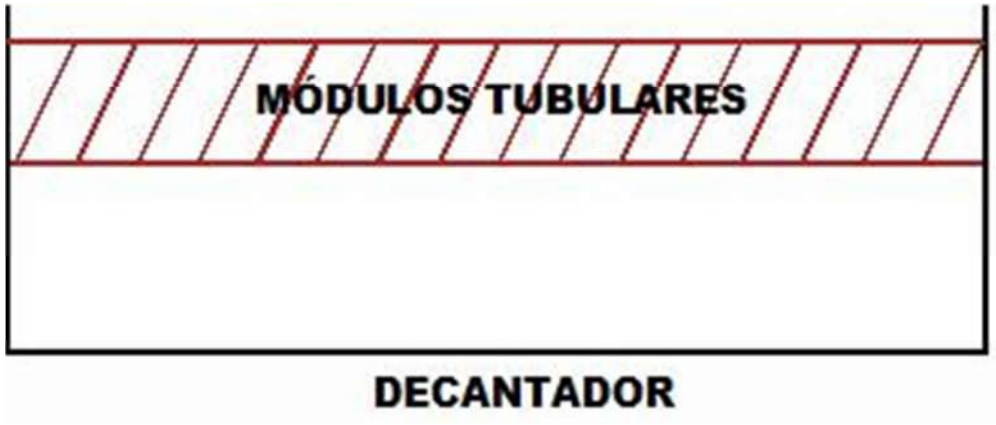
3.4. Decantação

A decantação é um fenômeno físico natural e corresponde a etapa de deposição das impurezas, aglutinadas em flocos no processo nas etapas anteriores do tratamento da água (coagulação e floculação), devido à ação da força gravitacional.

A deposição destes flocos no fundo do tanque de decantação, ou decantador, gera um resíduo denominado de lodo, e seu acumulo no decantador pode saturar o mesmo, ocasionando o aumento da turbidez de saída da água decantada. O lodo deve ser retirado periodicamente dos decantadores, afim de não comprometer o processo de decantação e consequentemente as etapas posteriores.

As análises de turbidez e cor da água de saída dos decantadores é um fator importante para se verificar a eficiência do processo de tratamento, porém, na ETA IV ainda não é feito este controle.

Figura 5 - Decantador.



Fonte: Autoria Própria.

3.5. Desinfecção

De acordo com as características da água bruta, do projeto da ETA e entre outros fatores, do tipo de desinfetante utilizado, faz se aplicação do desinfetante em pontos diferentes no tratamento. Na ETA IV esta dosagem é feita após a saída da água do decantador.

De acordo com Heller e Pádua (2010), “a desinfecção na água tem o objetivo de corrigir e prevenir. Este método busca eliminar os organismos patogênicos que possam estar presentes na água”.

A desinfecção pode ser realizada por dois tipos de agentes: o físico e o químico. Dentre os agentes físicos destacamos a luz solar, o calor e a radiação ultravioleta. Já a gama de agentes químicos é bem maior: ozônio, peróxido de

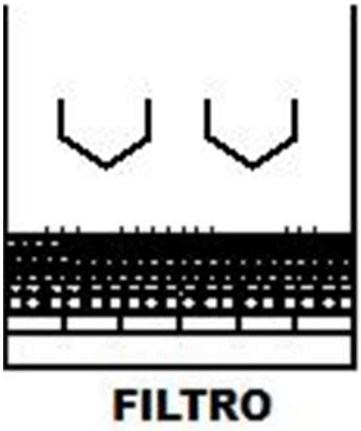
hidrogênio, permanganato de potássio, cloro, dióxido de cloro, hipoclorito de sódio, hipoclorito de cálcio, e diversos outros derivados clorados.

O DAE barbarense utiliza atualmente como agente desinfetante o hipoclorito de sódio, fornecido na forma líquida (>10% de cloro ativo), que é dosado na água através de equipamentos acionados manualmente e controlados por inversores de frequência. A dosagem do desinfetante deve ocorrer obedecendo à legislação vigente, observando um determinado residual que é controlado através de análise feita pelo operador da estação.

3.6. Filtração

Após a desinfecção a água é encaminhada aos filtros, onde ocorre o processo de filtração. Um filtro é constituído de um meio poroso granular, normalmente areia, de uma ou mais camadas, instalado sobre um sistema de drenagem, capaz de reter e remover as impurezas ainda presentes na água. No caso da ETA em questão, os filtros são formados por areia e carvão antracito.

Figura 6 - Filtro.



Fonte: Autoria Própria.

Além da remoção do restante das partículas em suspensão, no caso desta ETA, nos filtros ocorrem também a remoção de parte da carga bacteriana e a oxidação dos metais, devido à dosagem do desinfetante anteriormente a esta fase.

Sendo esta a etapa final do processo de clarificação em uma ETA convencional, é o filtro que determinará a qualidade do produto final, ou seja, da água. Após certo tempo de funcionamento, que é denominado de carreira de filtração, há a necessidade da lavagem do filtro, que é feita aplicando água no sentido contrário à filtração, com velocidade relativamente alta para que as impurezas retidas sejam retiradas.

3.7. Correção do pH

A correção do pH é efetuada através da adição de produtos químicos para que a água não se torne excessivamente ácida e tampouco excessivamente alcalina, mantendo-se dentro dos padrões de potabilidade. A acidez possibilita a corrosão de tubulações e equipamentos, enquanto a água abundantemente alcalina pode provocar incrustações nas tubulações.

Como dito no item 3.2.1., a ETA IV trabalha com pH em torno de 6,4 e 6,8, e após sair dos filtros faz-se necessária novamente a dosagem de um agente alcalinizante para que este pH chegue em torno de 7,0 e 7,2, considerado ideal para as redes de distribuição barbarenses.

Para este ajuste do pH utilizamos também o hidróxido de cálcio em suspensão aquosa, feito através de bombas dosadoras controladas manualmente e acionadas por inversores de frequência, e após análise, o operador faz a correção se necessário.

3.8. Fluoretação

Na ETA IV, após receber o alcalinizante a água recebe através de bomba dosadora controlada e acionada manualmente, uma pequena quantidade do Ácido Fluorsilícico na forma líquida (> 20% de concentração) única e exclusivamente para obedecer à exigência do Ministério da Saúde, um residual difícil de ser controlado pelo operador.

> A fluoretação, que não é considerada uma forma de tratamento, corresponde a adição de flúor, em geral na forma de ácido fluorsilícico, fluorsilicato de sódio, fluoreto de sódio ou fluoreto de cálcio, com a finalidade de prevenir a decomposição dos esmaltes dos dentes (HELLER; PADUA, 2010).

3.9. Demais variáveis do tratamento de água

As variáveis de um sistema de tratamento de água são diversas e não se pode ter controle sobre todas elas. Para que a água possa sair da ETA, dentro dos padrões de potabilidade, uma série de medições deve ser efetuada em cada etapa do processo, utilizando-se de reagentes químicos, equipamentos mecânicos e equipamentos eletrônicos, dependendo da variável a ser mensurada. Porém, graças à evolução tecnológica, temos hoje uma vasta gama de equipamentos automatizados que podem garantir a fluência do processo com o mínimo de intervenção humana, garantindo a tão desejada homogeneidade do produto final: a água potável. As variáveis que serão explanadas a seguir são de fundamental importância no que tange à operação de uma ETA convencional.

Vazão: A vazão de uma ETA é a quantidade de água que a mesma pode tratar em um determinado período de tempo, e pode ser expressa em l/s (litros por segundo). Os sistemas de bombeamento de água bruta, não são lineares, ou seja, a vazão de entrada em uma ETA pode sofrer variações. Como a dosagem do coagulante deve ser feita de acordo com a vazão, e também em função da turbidez e cor, um medidor de vazão inteligente deveria otimizar o processo de tratamento.

Turbidez – A turbidez na água é causada por partículas em suspensão, tais como argila, detritos sílicosargilosos, partículas orgânicas e inorgânicas finamente divididas, compostos orgânicos solúveis (dissolvidos) coloridos e outros microrganismos. De maneira genérica, podemos dizer que a turbidez é a quantidade de sujeira na água. É expressa em UT (unidade de turbidez), e juntamente com a vazão e a cor, determinam a quantidade de coagulante a ser dosado na água bruta. Já existe no mercado, instrumentos inteligentes para a medição de turbidez.

Cor - Cor na água é o resultado da presença de íons metálicos naturais como ferro ou manganês, de restos de vegetais ou de resíduos industriais, entre outros, dissolvidos na água. É expressa em PtCo (platina cobalto) e juntamente com a turbidez forma todas as impurezas presentes na água.

4. AUTOMAÇÃO

Automação (do latim *Automatus*, que significa mover-se por si) pode ser definida como a aplicação de técnicas, *softwares* e/ou equipamentos específicos em um determinado processo, com o objetivo de aumentar a sua eficiência reduzindo consumo de energia e/ou matérias primas e gerando melhores condições de segurança, seja material, humana ou das informações referentes a esse processo, ou ainda, de reduzir o esforço ou a interferência humana sobre esse processo.

Silveira (1998 *apud* FONSECA, 2009 p. 1) descreve a automação como sendo “um conceito e um conjunto de técnicas por meio das quais se constroem sistemas ativos capazes de atuar com uma eficiência ótima pelo uso de informações recebidas do meio sobre o qual atuam”.

O processo de automatização de uma ETA inicia-se pelo nível hierárquico mais baixo, ou seja, pelos transdutores - equipamentos que transformam grandezas não elétricas em grandezas elétricas, como exemplo, monitores de cloro residual, turbidez e coagulante.

Os CLPs (Controlador Lógico Programável) - equipamentos que recebem as informações dos transdutores - executam a lógica obedecendo rigorosamente a um *software* instalado e a condições preestabelecidas.

Os transdutores têm a responsabilidade de transmitir os sinais das variáveis do processo para os atuadores de processo. Os atuadores são os dosadores de produtos químicos, controladores de válvulas e de outros dispositivos de acionamento, ou seja, são equipamentos que atuam diretamente no processo de tratamento.

4.1. Instrumentação

A instrumentação é um dos recursos mais importantes da automação, pois proporciona os meios para a medição das condições do processo e de grande parte dos atuadores, visando à homogeneidade do desempenho, a fim de garantir uma operação mais segura e a redução do custo global. Entretanto, os sistemas de saneamento utilizam diversos instrumentos de medição convencional, ou seja, instrumentos que não possuem nenhuma forma de processamento do sinal medido.

De modo geral, esse tipo de topologia pode tornar o sistema de automação indisponível, exigir excessiva manutenção e deixar de gerar diagnósticos avançados, dificultando a tomada de decisão mais adequada. Além disso, esses sinais estão sujeitos às interferências eletromagnéticas, pois são transmitidos de forma analógica, em sinal de corrente padrão de 4 – 20 mA, por exemplo.

Assim sendo, a fim de garantir a qualidade do sinal medido com vistas à otimização operacional e ao aperfeiçoamento da gestão do processo, surge a instrumentação inteligente como alternativa eficiente aos métodos tradicionais de arquitetura de instrumentação na automação dos sistemas de abastecimento de água.

4.1.1. Instrumentação Inteligente

Podemos definir instrumentação inteligente como o conjunto de técnicas e dispositivos usados para observar, medir, registrar fenômenos físicos e efetuar ações com maior confiabilidade, com conectividade com outros equipamentos e dispositivos, e com capacidade de manipular as grandezas observadas, visando a sua análise e processamento.

A comunicação visa à transferência de informações e reprogramação destas nos instrumentos, e a confiabilidade destas ações é obtida através de recursos internos de autoavaliação e ajuste.

Os principais elementos de um Instrumento Inteligente (II) estão representados na Figura 7. Neste sistema observa-se que o transdutor converte o sinal ou grandeza normalmente não elétrica (VM) em grandeza elétrica equivalente (S).

Figura 7 – Elementos de um instrumento inteligente.

Fonte: Autoria Própria.

Como S nem sempre possui amplitude adequada ou compatibilidade com os demais dispositivos, é necessário modificá-la por meio de condicionamento, para que o sinal (SM) possa ser utilizado nos dispositivos de manipulação.

Os dispositivos de manipulação, geralmente empregados para supervisionar e controlar processos, podem ser interfaces de um CLP (Controlador Lógico Programável), interfaces com computador ou interfaces com microprocessador. Este sistema pode ser analógico, mais antigo e com dispositivos muito simples, ou digital, de geração mais recente. As principais vantagens dos sistemas digitais são: a gama praticamente ilimitada de transferências possíveis; a simplicidade de projeto; a calibração; a invariabilidade no tempo; a ausência de interferências e a possibilidade de criação de sistemas autoajustáveis com autodiagnóstico.

4.2. Monitor de coagulação

O monitor de coagulação é um equipamento que mede a carga elétrica residual líquida na água. Como a água bruta apresenta carga elétrica negativa e o coagulante fornece a carga positiva, é possível a utilização deste monitor de coagulação inteligente, ou zetômetro, para um controle eficiente da coagulação. É necessário fornecer ao instrumento um ponto de referência que representa um padrão ótimo de qualidade de água coagulada.

Figura 8 - Monitor de coagulação.

Fonte: Digimed (2015).

Este ponto de referência é obtido a partir da realização de testes e é utilizado para ajuste do zero do instrumento. Valores de fluxo de corrente acima do ponto de referência indicam que há excesso de coagulante e valores abaixo indicam uma dosagem insuficiente. A partir da referência fornecida ao instrumento, cria-se uma janela de operação na qual ele consegue visualizar alterações na qualidade da água bruta agindo de modo inteligente sobre a coagulação e fazendo o ajuste de dosagem automaticamente, enviando o sinal necessário ao inversor de frequência da bomba dosadora de coagulante.

4.3. Turbidimetro

O Turbidimetro é um equipamento que faz a medição da turbidez da água, através da dispersão de luz de um ponto a outro, ou seja, é um método de medida da redução da transmissão de luz em um meio, causada pelas partículas em suspensão. Ela é determinada graças a um sistema ótico que mede a absorbância de um raio luminoso que atravessa a suspensão.

Figura 9 - Turbidimetro.

Fonte: Digimed (2015).

Tal equipamento quando possui certa tecnologia embarcada, além de converter e enviar sinais a um sistema supervisório pode fazer sua limpeza e calibração automaticamente. Os pontos a receberem o controle de turbidez são a água bruta, saída do decantador e a água tratada.

4.4. Analisador de cor

O analisador de cor é um aparelho que mede a cor aparente da água através do método colorimétrico ou espectrofotômetro. O método colorimétrico pode ser definido como a quantificação física e/ou psicológica do fenômeno de percepção de cores pelos seres humanos, e é utilizado em alguns equipamentos de medição, inclusive eletrônicos. Já a espectrofotometria é o método mais utilizado nas análises físico-químicas. O espectrofotômetro é um instrumento que permite comparar a radiação absorvida por uma solução que contém uma quantidade desconhecida de um determinado soluto, e outra com uma quantidade conhecida da mesma substância.

Figura 10 - Analisador de cor - Colorímetro.

Fonte: Digimed (2015).

A cor das substâncias se deve a absorção (transmitância) de certos comprimentos de ondas da luz branca que incide sobre elas, deixando transmitir aos nossos olhos apenas aqueles comprimentos de ondas não absorvidos.

Todas as substâncias podem absorver energia radiante, mesmo o vidro que parece completamente transparente absorve comprimentos de ondas que pertencem ao espectro visível. A água absorve fortemente na região do infravermelho. Quando a luz atravessa uma substância, parte da energia é absorvida (absorbância), podendo ser medida, então, eletronicamente.

Um analisador de cor inteligente além de interligar-se na rede de dados, também pode fazer sua limpeza e calibração automaticamente. Os pontos de monitoração de cor são a água bruta, saída do decantador e água tratada.

4.5. Controlador de pH

O medidor de pH, ou pHmetro, é o aparelho que faz a medição do pH nas amostras de água analisadas geralmente através de eletrodo. A quantidade de íons H^+ desenvolve certo potencial elétrico, tornando-se mensurável.

Figura 11 - Controlador de pH.

Fonte: Digimed (2015).

Para que haja uma coagulação ótima, o pH é peça fundamental neste processo, sendo uma das principais variáveis. Com a utilização de um controlador inteligente de pH, podemos atrela-lo ao sistema e utilizar o sinal gerado pelo mesmo

para fazer o controle do inversor de frequência ligado à bomba dosadora de alcalinizante, tornando a dosagem automatizada, segura e controlada.

Com a utilização do zetômetro, haverá variações de dosagem de coagulante, porém, o controlador de pH inteligente fará a correção deste pH para manter a homogeneidade da água coagulada.

O pH é essencialmente importante em qualquer processo químico, assim como é o tratamento da água. Além do pHmetro da coagulação, há necessidade de se implantar mais dois pHmetros, um para a monitoração do pH da água bruta e outro para o controle do pH da água tratada, uma vez que, como exposto no item 7 do capítulo 3, há de se fazer a correção final do pH da água após a mesma passar pelo processo de filtração.

4.6. Analisador de Cloro

O analisador de cloro é um equipamento que monitora o valor de cloro residual na água, importantíssimo para a correta desinfecção e oxidação das impurezas presentes na água. Com o funcionamento semelhante ao analisador de cor, um reagente químico é adicionado à amostra a ser analisada e de acordo com a quantidade de cloro disponível, a reação química ocorre e a amostra torna-se mensurável. Atrelando um analisador de cloro inteligente ao sistema de tratamento, podemos controlar os inversores de frequência das bombas dosadoras, e com isso, manter o *set-point* (valor alvo) correto de dosagem do desinfetante utilizado na ETA.

Figura 12 - Analisador de Cloro.

Fonte: Digimed (2015).

4.7. Analisador de flúor

O analisador de flúor faz a medição dos íons de flúor presentes na água. Geralmente a medição ocorre através de dois métodos distintos: eletroanalítico e colorimétrico. O método colorimétrico funciona semelhantemente ao analisador de cloro, onde um reagente é adicionado alterando a coloração da amostra a ser analisada e posteriormente passando por um colorímetro. Já o método eletroanalítico funciona de maneira similar a um pHmetro, com um eletrodo medindo o potencial elétrico.

Figura 13 - Analisador de Flúor.

Fonte: Digimed (2015).

5. REDES

Comunicação sempre foi uma necessidade humana, buscando aproximar comunidades distantes. Sinal de fumaça, pombo-correio, telégrafo e telefone, são exemplos de comunicação. A evolução tecnológica trouxe até nós os computadores e cada vez mais a necessidade de comunicação.

Uma rede de computadores é um conjunto de *hardware* e *software* que permite o estabelecimento da comunicação entre computadores. Os instrumentos inteligentes citados no capítulo anterior, nada mais são que computadores, exercendo atividades à que são programados. Então, para interligar estes computadores a uma rede que leve a informação até outro computador para monitoração, armazenamento, e/ou qualquer outro tipo de atividade, necessitamos das redes de computadores.

Em processos de pequeno porte, um controlador isolado pode suprir as necessidades. No entanto, em processos mais complexos, os subprocessos são interdependentes e os controladores não podem trabalhar isoladamente, devendo ser interligados para trocar as informações. Assim sendo, os equipamentos de um sistema de automação são interligados em redes que podem possuir diversos tipos de arquitetura, conforme exemplos descritos em seção futura deste trabalho.

5.1. Modelo de Sete Camadas OSI

A OSI (*Open System Interconnection* - Interconexão de Sistema Aberto) é um conjunto de normas definidas pela ISO (*International Standard Organization* - Organização de Padronização Internacional), que por meio da ISO 7498, estabeleceu os padrões para elaboração de protocolos de comunicação entre dois ou mais computadores. Uma das partes da OSI é o modelo de sete camadas de comunicação. Cada uma das camadas representa um processo de codificação e decodificação dos dados para transmissão em uma rede.

A maioria dos protocolos existentes no mercado segue o modelo OSI, mas muitas vezes apenas algumas camadas são utilizadas. Isso acontece porque o modelo foi elaborado para suprir as necessidades de uma rede bastante complexa,

mas apenas os níveis 1, 2 e 7 são necessários na automação. A Figura 14 representa as sete camadas do modelo OSI.

Figura 14 - Camadas OSI.

Fonte: Autoria Própria.

Acima da camada de aplicação encontra-se o programa de usuário, que consiste em um aplicativo que vai gerar a mensagem a ser conduzida e protocolada na rede de comunicação. É importante salientar que a estrutura do modelo OSI é constituída de uma arquitetura hierárquica, disposta em níveis. Cada nível presta um serviço para um nível mais baixo, com certa confiabilidade. Abaixo do nível de comunicação encontra-se o meio de transmissão de dados. A seguir, cada camada (nível) do modelo de referência OSI é explicada em detalhes.

Camada 1 - Física: esta camada define o meio físico de comunicação dos dados. É uma camada necessária em todos os protocolos de comunicação, pois nela se incluem as funções de ativar, manter e desativar a conexão física. Efetua a leitura da mensagem e gera os sinais para a interface física do meio externo à

comunicação. Define, portanto, características elétricas, como níveis de tensão e corrente, entre outros; características mecânicas, como dimensões dos conectores, número de pinos, bitola e impedância de cabos ou de fibra ópticas, entre outras especificações; características funcionais, como controle; e de procedimentos, como comando e gerenciamento.

Camada 2 - Enlace: situa-se na conexão entre dois pontos de uma rede, e é onde são feitas as formatações das mensagens e os endereçamentos dos pontos em comunicação. Este nível possui o conjunto de regras que governa a troca de dados através do meio físico entre dois pontos. Assegura que o conteúdo da mensagem, gerada em sua origem, seja exatamente igual ao conteúdo da mensagem que chega ao local de destino. Para tal, essa camada possui uma sub-rotina, muitas vezes constituída por um algoritmo especial, que permite a detecção de erros de comunicação no nível da camada física, mantendo a integridade da mensagem.

Camada 3 - Rede: cuida da rede, achando um meio mais adequado de transporte da mensagem. Agrega ou modifica os endereços na mensagem ao longo da rede. Possui, portanto, a função de endereçamento de forma a promover todo o roteamento, como o roteamento dos dados entre os nós para atingir o endereço por meio de seus recursos.

Camada 4 - Transporte: possui como função principal o controle de fluxo, estabelecendo a melhor maneira de transporte das mensagens na rede. Além de assegurar que as mensagens cheguem de forma ordenada ao seu local de destino, estabelece o tamanho do bloco em que elas serão enviadas, fatiando-as de tal modo que sua chegada dar-se-á por meio de uma determinada sequência dentro de uma numeração especifica. O nível quatro, ao contrário dos níveis anteriores que atuam em segmentos de rede, opera entre duas pontas finais que estão se comunicando entre si, por exemplo, o computador da matriz da empresa e o computador da filial.

Camada 5 - Sessão: responsável pelo estabelecimento da conexão, maneja e sincroniza as conexões entre dois processos, estabelecendo uma senha ou ficha de acesso para o pronto estabelecimento da sessão de comunicação. É um procedimento semelhante àquele em que dizemos alô para iniciar uma comunicação telefônica. As regras para a troca das mensagens dentro da especificação procedural são negociadas entre as partes, ou seja, define-se quem deve falar primeiro e se as partes devem enviar e receber dados simultaneamente ou não.

Camada 6 - Apresentação: esta camada é responsável pela forma de apresentação do código da mensagem, ou seja, possui a função de converter o código dentro da especificação lógica do sistema. Assegura que a mensagem seja recebida e devidamente interpretada pelo sistema especialista do receptor. Portanto, garante a sua compatibilidade. No caso da criptografia, os dados são codificados no nível de apresentação do transmissor e decodificados no nível de apresentação do receptor.

Camada 7 - Aplicação: este nível é definido pela aplicação final do usuário, que são os processos que utilizam as redes. São, por exemplo, os programas aplicativos do usuário, as transações que rodam no seu terminal, bancos de dados distribuídos e aplicativos de redes locais. Nesta camada, cada estação envia e recebe mensagens pela rede, codificadas em um formato específico em que cada parte da mensagem tem um significado pré-definido de acordo com a linguagem da aplicação. O *software* aplicativo, instalado numa estação que esteja enviando dados, deve montar a mensagem utilizando esta linguagem para solicitar e enviar informações de ou para outras estações. A estação que recebe os dados deve interpretar a mensagem de acordo com a mesma linguagem e responder adequadamente às solicitações recebidas.

5.2. Arquitetura

Arquitetura, neste contexto, é a forma de interligação entre os componentes de um sistema de automação. Os tipos de arquitetura mais comuns são as centralizadas e as distribuídas.

Arquitetura Centralizada: é aquela em que todos os sinais de campo vão para uma única sala de controle, onde trabalham controladores e operadores. Este tipo de arquitetura está deixando de ser utilizado, devido aos altos custo e risco de acidentes na sala de controle, o que causaria a parada total do sistema.

Arquitetura Distribuída: neste tipo de arquitetura os controladores ou módulos de entrada e saída ficam próximos ao processo, reduzindo o custo de cabeamento até os instrumentos e atuadores. Os controladores e os módulos de entrada e saída são interligados em rede para trocar informações entre si e com o

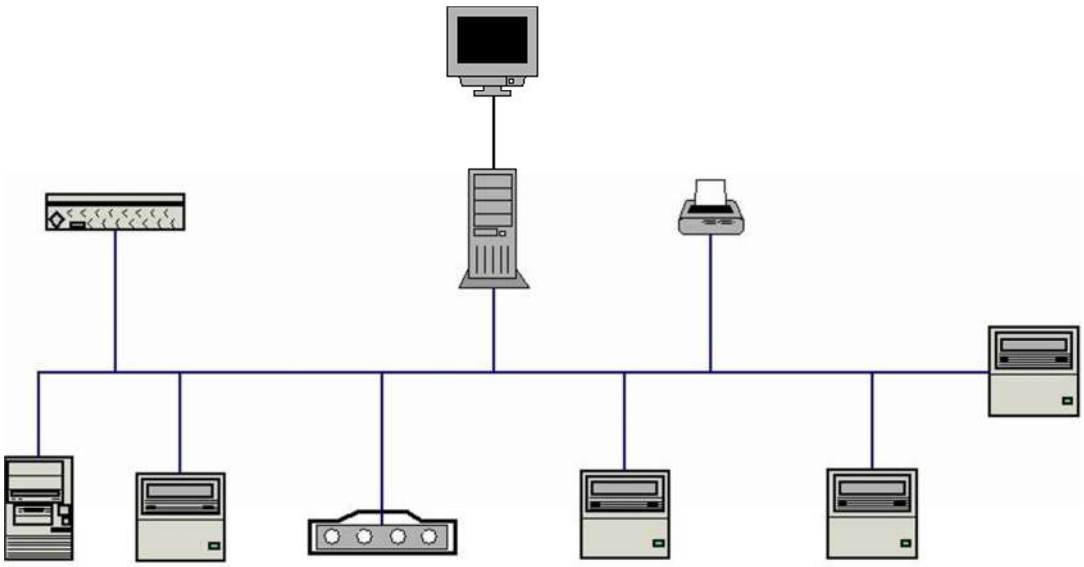
sistema de supervisão. Se um controlador ou módulo de entrada e saída apresentar defeito, apenas uma pequena parte do processo será prejudicada.

Rede em Anel: nesta arquitetura os controladores ou módulos de entrada e saída são interligados de forma que os dados trafeguem sequencialmente, de um dispositivo para o próximo. Nesta rede, há dois tipos possíveis de anéis.

- **Anel físico:** quando cada trecho do cabo de comunicação interliga somente dois módulos sequenciais, de forma que o conjunto seja um caminho, ou anel, fechado.
- **Anel lógico:** quando outra forma de interligação física é utilizada, mas os dados circulam sequencialmente entre os módulos sempre na mesma ordem. Diversas redes de chão de fábrica utilizam este método.

Rede em Barramento: nesta forma de comunicação os equipamentos são interligados uns aos outros em forma de barramento, ou seja, todos têm condições de se comunicar entre si, pois estão ligados ao mesmo conjunto de cabos. A comunicação é serial e obedece aos padrões físicos da rede e aos padrões lógicos do protocolo adotado. As redes *Ethernet*, *Profibus*, CAN (*Controller Area Network*) e todas as redes baseadas no padrão RS-485 são interligadas em barramento.

Figura 15 - Equipamentos interligados em rede de barramento.



Fonte: Autoria Própria.

Rede em Estrela: nesta topologia todas as estações são ligadas a um único ponto central, normalmente um *switch* (chaveador que separa as seções lógicas da rede). Logicamente, todos os nós da rede estão interligados, mas cada ponto de conexão do *switch* é eletricamente isolado dos demais. Isto permite isolar os defeitos que possam ocorrer em uma única estação sem que o restante da rede seja comprometido.

Cada conexão de *switch* é chamada de segmento. Cada segmento pode possuir um único dispositivo conectado ao próprio segmento ou vários dispositivos conectados em estrela, barramento ou anel. Quando um ou mais segmentos estão interligados em estrela, a rede correspondente é chamada de **rede em árvore**.

5.3. Redes de Campo

Na definição do ISA (*Instrument Society of America*) o *fieldbus*, ou barramento de campo, é uma linha de comunicação serial, digital, bidirecional, de acesso compartilhado para interligação dos dispositivos primários de automação. Inclui transmissores/sensores, atuadores e outros dispositivos simples, com capacidade de processamento local, instalados na área de campo com os dispositivos de controle e automação de nível imediatamente superior. O IEEE (*Institute of Electrical and Electronics Engineers*) apresenta-o como um “barramento para interligação generalizada de dispositivos simples, usados em instrumentação, controle de processos e automação industrial”.

As necessidades dos usuários são as mais diversas possíveis, portanto, a fim de atendê-las, os sistemas de automação são interligados rotineiramente aos níveis hierárquicos mais elevados da informática industrial e empresarial. Os dados oriundos do campo, a partir dos SDCD (Sistemas de Controle Digital Distribuído), CLPs e similares passam a ser integrados a outros bancos de dados de gestão.

A maioria dos controladores existente no mercado permite a interligação em rede e a maioria dos fabricantes e usuários começaram a utilizar a rede *Ethernet* como padrão informal, até que esta acabou por se tornar um padrão de fato. A *Ethernet* é uma rede de alta velocidade, de 10 ou 100 Mbps (*Megabit* por segundo), muito usada na automação de escritórios, com diversos meios físicos, menor custo,

fácil instalação e gerenciamento e bastante conhecida e dominada pelo mercado de informática.

No entanto, isto não garante a comunicação entre controladores de vários fabricantes interligados a uma rede *Ethernet*. A razão disso é que apesar de a *Ethernet* sempre utilizar os protocolos TCP/IP (*Transmission Control Protocol/Internet Protocol* - Protocolo de Controle de Transmissão/Protocolo de Internet) na camada de enlace, as camadas de aplicação podem possuir dezenas de protocolos diferentes.

5.4. Tipos de protocolo

RS232-C: Protocolo ponto a ponto, com distância máxima de 15m entre as estações e taxa de transmissão de no máximo 115 kbps. Existem dois caminhos de dados independentes e em sentidos opostos neste meio, o que permite que as duas estações transmitam e recebam simultaneamente (mecanismo conhecido como *full-duplex*). Normalmente, este protocolo é utilizado para conexão de equipamentos de programação ou para interligar um equipamento a um modem ou conversor de protocolos (*gateway*). Apenas as camadas físicas e de enlace estão definidas para este protocolo. A aplicação deve ser desenvolvida caso a caso.

RS485: Protocolo ponto/multiponto com velocidade máxima de 115 kbps e distância máxima de 1200 m. No máximo 32 estações podem participar de cada linha, mas com o uso de repetidores, até 256 estações podem ser endereçadas. Pode funcionar em configurações *half-duplex* ou *full-duplex*. Os nós são passivos, bastando interligar todas as estações da rede em paralelo. Esta especificação inclui a camada física e de enlace e, opcionalmente, uma camada padronizada de aplicação (Protocolo ASCII (*American Standard Code for Information Interchange*)). Graças à simplicidade de configuração, este protocolo é bastante utilizado em sistemas de aquisição de dados. O meio físico RS485 é utilizado como base na maioria das redes de automação.

IEC61158: Protocolo criado pela IEC (*International Electrotechnical Commission*) para comunicação entre instrumentos, utilizando os mesmos cabos normalmente utilizados para transmissão de sinais analógicos. O meio físico baseia-se em um *loop* de 0 a 20 mA com o sinal sendo modulado em tensão. A

especificação possui também uma camada de enlace com mecanismos mestre/escravo, produtor/consumidor e *publisher/subscriber*. Esta norma é utilizada como base em redes HART (*Highway Addressable Remote Transducer*), *Fieldbus Foundation* e *Profibus*.

***Controller Area Network* (CAN):** Rede desenvolvida pela Bosch para interligar equipamentos inteligentes em aplicações automotivas ao computador de bordo, por exemplo, sistemas de injeção eletrônica, ignição eletrônica, freios ABS, ar-condicionado e sensores de temperaturas e pressão de água e óleo. Apenas a camada de enlace é padronizada e se baseia no mecanismo produtor/consumidor. A camada física e de aplicação devem ser desenvolvidas caso a caso. Uma associação de fabricantes foi criada para incentivar a aplicação da rede CAN em automação industrial, a CIA (*CAN in Automation*).

***DeviceNet*:** Implementação da CAN, desenvolvida pela *Rockwell Automation*. Foi transformada em norma internacional — IEC 62026. A *DeviceNet* é uma rede de baixa capacidade, destinada à comunicação entre dispositivos discretos e CLPs ou computadores. Tem como principal característica a alta imunidade a ruídos e vibrações obtida graças à sua padronização física. O controle de acesso ao meio é baseado no mecanismo produtor/consumidor, mas podem-se utilizar também os mecanismos mestre/escravo, *Token-Passing* ou mesmo sistemas mistos. A taxa de transmissão varia entre 125 kbps a 500 m e 500 kbps a 100 m. É possível endereçar até 64 nós. A camada de aplicação permite a existência de dispositivos inteligentes.

***Profibus*:** Padrão definido pela norma alemã DIN (*Deutsche Industrienorm*) 19245 e pelas normas europeias EN (European Normes) 50170 e EN 50254. Possui mecanismo misto de acesso ao meio, mas o acesso para a comunicação entre estações de controle é através de *Token-Passing*. Utiliza o mecanismo mestre/escravo para comunicação entre estações de controle, dispositivos e instrumentos. Vários meios físicos podem ser utilizados. O meio principal é o RS-485 com velocidades entre 9,6 kbps a 1200 m e 115 kbps a 100 m. Este padrão também pode utilizar *Ethernet*, fibra óptica e IEC61158-2 como meio físico As distâncias máximas variam de acordo com este meio. O número máximo de participantes em cada linha, incluindo repetidores, é de 32 nós, e uma rede pode ter um total de até 125 participantes. Há dois tipos de camadas de aplicação no *Profibus*: *Decentralized Periphery* (DP) utilizada em controladores programáveis e dispositivos, e *Process Automation* (PA) utilizada para formar redes de instrumentos e atuadores

inteligentes. O *Fieldbus Message Specification* (FMS) permite a utilização de instrumentos inteligentes e realiza a distribuição de controle e programação dos dispositivos por meio de blocos funcionais.

***Foundation Fieldbus*:** Padrão internacional definido pela IEC e ISA e administrado pela *Fieldbus Foundation*. Assim como o *Profibus*, também é um padrão de chão de fábrica utilizado para interligar instrumentos, atuadores e controladores. Dois meios físicos são possíveis: O *Fieldbus* H1 usa meio físico e enlace definidos na IEC61158 e utiliza os mecanismos produtor/consumidor e mestre/escravo. O *Fieldbus High Speed Ethernet* (HSE) utiliza rede *Ethernet* de alta velocidade (100 Mbps) como meio físico e a mesma camada de enlace do H1. Através do FMS, podem-se programar aplicações distribuídas entre todos os participantes da rede.

***Modbus*:** Criada pela *Modicon,* era inicialmente uma rede proprietária utilizada na comunicação entre CLPs e remotas de telemetria da própria empresa, mas no final da década de 80 sua especificação foi aberta e colocada em domínio público. Hoje, uma grande variedade de equipamentos possui esta interface, entre eles, CLPs, instrumentos, controladores de malha fechada, acionamentos, medidores, remotas, etc. O meio físico da rede *Modbus* é o RS485. Até 256 estações podem se comunicar a 9,6 kbps em distâncias de até 1200 m. O controle de acesso ao meio é mestre/escravo e a camada de aplicação é bastante simples podendo ser implementada sem dificuldade até por programadores pouco experientes. É uma boa opção de baixo custo para a comunicação com baixas taxas de transmissão.

***Interbus*:** Rede desenvolvida pela *Phoenix Contact*, hoje aberta a empresas que aderiram ao *Interbus Club*. Além disso, a *Phoenix* possui uma variedade de interfaces que permitem integrar CLPs de diversos fabricantes à rede. No *Interbus*, o mecanismo de acesso ao meio é chamado de registrador de deslocamento lógico. Isto significa que os dados de todas as estações da rede são transmitidos conjuntamente em uma única operação. O controlador mestre da rede sincroniza e controla o fluxo. Este método permite otimizar o tempo de rede, pois apenas uma pequena parcela da comunicação é ocupada por bits de controle. A taxa de transmissão é de 500 kbps. As estações, em número máximo de 512, são ligadas em anel. Não é necessário endereçar os módulos, pois a sequência das estações no anel define o destino e origem dos dados.

***Actuator Sensor Interface* (ASI):** Rede de dispositivos de baixa capacidade, tem como característica mais importante seu meio físico, um cabo chato autossustentável, com proteção contra interferências eletromagnéticas que é lançado na área dos dispositivos discretos. A conexão dos nós pode ser feita de forma simplificada, pois o conector envolve o cabo e faz o contato elétrico sem necessidade de nenhuma ferramenta. No entanto, a rede tem capacidade muito baixa. Cada nó possui apenas 4 bits de entrada e 4 bits de saída e só é possível endereçar 32 nós. Por este motivo, normalmente é usada em conjunto com *Profibus* apenas no nível de dispositivos; a comunicação é mestre-escravo a uma taxa máxima de transmissão de 168 kbps.

***Ethernet*-TCP/IP:** O conjunto de protocolos TCP/IP, desenvolvido para implementar as camadas de enlace e rede e redes locais, posteriormente tornou-se a base para o funcionamento da internet. Devido à falta de um padrão de rede para automação, de seu baixo custo e total padronização, a *Ethernet*-TCP/IP tornou-se o padrão informal em sistemas de automação. Entretanto, não é a melhor opção porque o método de acesso ao meio do protocolo TCP (camada de enlace) utiliza o mecanismo de controle de acesso ao meio CSMA-CD (*Carrier Sense Multiple Access with Collision Detection*). Esta tecnologia permite a construção de redes com topologias complexas com um número extremamente alto de participantes (o protocolo IPv4 pode endereçar mais de 4 bilhões de estações). As taxas de transmissão vão até 100 Mbps.

A *Open DeviceNet Association* (ODVA) desenvolveu o protocolo *Ethernet*/IP que utiliza o endereçamento IP e as altas taxas de transmissão da *Ethernet*; mas em vez do protocolo de controle de acesso TCP, utiliza o método de enlace produtor/consumidor do CAN e a camada de aplicação da *DeviceNet*.

6. ASSEGURANDO A INFORMAÇÃO

A informação sempre foi um dos bens mais importantes de uma organização, porém, outrora as informações mais críticas para uma empresa poderiam ser guardadas e trancadas dentro de uma gaveta. A evolução tecnológica dizimou grande parte dos papéis que uma empresa trancava, digitalizando a maioria dos documentos. Para protegermos estes dados devemos saber que este não é somente um assunto de tecnologia, mas deve ser uma decisão empresarial.

Confidencialidade, Integridade e Disponibilidade formam a tríade CIA (*Confidentiality, Integrity and Availability*), e são os principais atributos da segurança da informação, orientando a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Outros atributos importantes são a autenticidade, a irretratabilidade, e a conformidade.

- **Confidencialidade:** é a propriedade que garante que o acesso à informação seja obtido somente por pessoas autorizadas;
- **Integridade:** é garantir que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
- **Disponibilidade:** é o atributo de garantia que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- **Autenticidade:** propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo;
- **Irretratabilidade:** atributo que garante a impossibilidade de negação da autoria em relação a uma transação anteriormente feita;
- **Conformidade:** garantia de que o sistema deve seguir as leis e regulamentos associados a este tipo de processo.

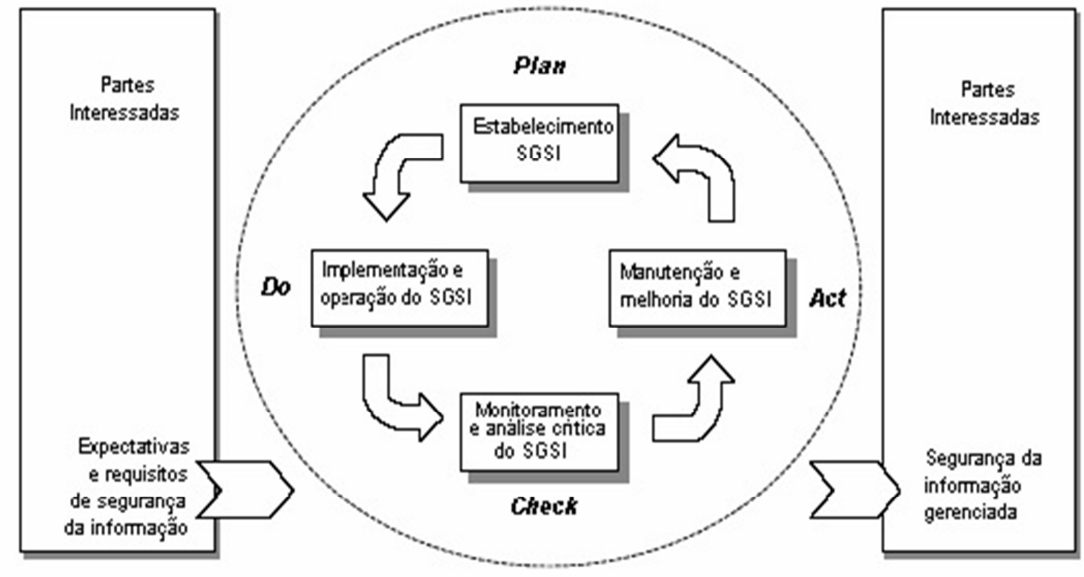
As ameaças à que as informações podem estar sujeitas, são de origem natural (fenômenos da natureza), involuntárias (ameaças inconscientes) ou voluntárias (propositais, causadas por agente humano). Já as vulnerabilidades,

podem ser as físicas (instalações fora do padrão), naturais (incêndios, tempestades, etc...), de *hardware* (obsolescência, mau uso), de *software* (obsolescência, configuração, instalação), comunicação (acesso não autorizado, perda de comunicação) ou humanas (treinamento, sabotagem, erros). Quanto às medidas de segurança, temos as preventivas (evitar o incidente), detectáveis (identificar possíveis condições e/ou indivíduos causadores de ameaças) e corretivas (correção de problemas já acontecidos ou detectados).

6.1. Gestão de Segurança da Informação

Um SGSI (Sistema de Gestão de Segurança da Informação) é parte de um sistema de gestão global da corporação. O foco de um SGSI é a gestão dos riscos aos negócios. A adoção de um SGSI deve ser uma decisão estratégica para uma organização, e a especificação e implementação do SGSI são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos empregados e tamanho e estrutura da organização.

Figura 16 - Modelo PDCA aplicado aos processos do SGSI.



Fonte: (ISO/IEC 27001, 2006).

A ISO/IEC 27001 faz abordagem de processo para estabelecer e implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI de uma organização. De acordo com esta ISO, o modelo a ser seguido é o PDCA (*Plan-Do-Check-Act*), que é aplicado para estruturar todos os processos do SGSI. A Figura 16 ilustra como um SGSI considera as entradas de requisitos de segurança de informação e as expectativas das partes interessadas, e como as ações necessárias e processos de segurança da informação produzidos resultam no atendimento a estes requisitos e expectativas.

6.2. Políticas de Segurança da Informação

Para a existência da PSI primeiramente devemos descrever a filosofia e as regras básicas para o uso do recurso informação, independente do ambiente em que esta esteja, deixando explicito o que cada pessoa da organização deve cumprir no que se refere à proteção da informação. A PSI não surge do nada, é necessário que esteja alinhada aos objetivos da organização. A partir dos objetivos do negócio se determina os objetivos da segurança da informação.

A principal recomendação é criar uma política principal, descrita em um documento curto e simples de forma que todos os usuários entendam facilmente como a organização deseja que a informação seja tratada e as responsabilidades dos usuários. Outros documentos mais específicos e normas devem ser criados como complemento.

Esse conjunto deve: Declarar e clarificar as regras; Definir obrigações, responsabilidades e autoridade; Formalizar processos e procedimentos; Documentar a boa cultura empresarial; Evitar o crescimento da parte do folclore organizacional que impede as boas práticas de proteção; Possibilitar seu uso em questões legais contratos, relacionamento com as pessoas e com o mercado; Estabelecer padrões; Ajudar a educar as pessoas; Ser a base para uma efetiva arquitetura de segurança da informação.

Devemos considerar em um planejamento de segurança da informação:

a) Características do Negócio;

b) Estrutura do negócio;

c) Plano estratégico de segurança;

d) Mapear as vulnerabilidades e priorizar as ações;

e) Identificar os recursos necessários;

f) Definir níveis de segurança.

Outro fator que devemos levar em consideração é que não há solução certa ou errada, e sim, mais ou menos adequada.

A política de segurança é que vai nortear todos os trabalhos a serem executados, como: Controle de Acesso; Sistema de Gestão de Segurança da Informação; Políticas de *Firewal*; e *Backup*.

6.3. Barreiras de Segurança

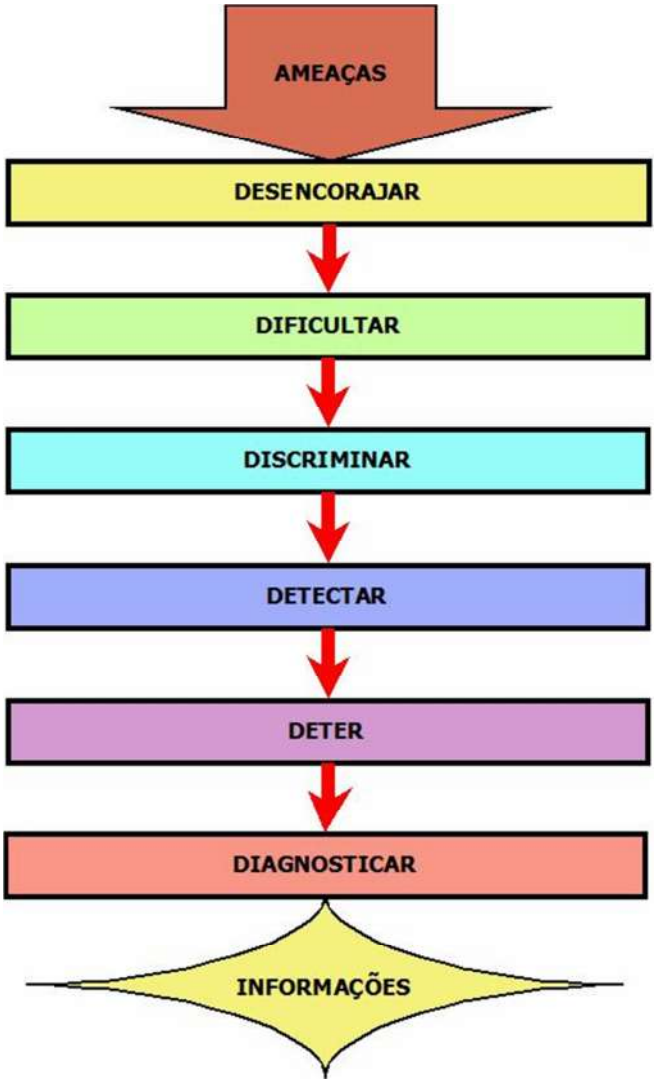
Conceitualmente, diante da amplitude e complexidade do papel da segurança, é comum estudarmos os desafios em camadas ou fases, particionando todo o trabalho para tornar mais claro o entendimento de cada uma delas. Neste caso, denominamos esta divisão de Barreiras de Segurança, onde cada uma delas tem participação importante no objetivo maior de reduzir os riscos à informação, e por isso, deve ser dimensionada adequadamente para proporcionar a mais perfeita interação e integração, como se fossem peças de um único quebra-cabeça.

A Figura 17 representa o diagrama das Barreiras de Segurança.

- **Desencorajar:** Esta é a primeira das cinco barreiras de segurança e cumpre o papel importante de desencorajar as ameaças. Estas, por sua vez, podem ser desmotivadas ou podem perder o interesse e o estímulo pela tentativa de quebra de segurança por efeito de mecanismos físicos, tecnológicos ou humanos. A simples presença de uma câmera de vídeo, mesmo falsa, de um aviso da existência de alarmes, campanhas de divulgação da política de segurança ou treinamento dos funcionários informando as práticas de auditoria e monitoramento de acesso aos sistemas, já são efetivos nesta fase.
- **Dificultar:** O papel desta barreira é complementar à anterior através da adoção efetiva dos controles que irão dificultar o acesso indevido. Como exemplo, podemos citar os dispositivos de autenticação para acesso físico, como roletas, detectores de metal e alarmes, ou lógicos,

como leitores de cartão magnético, senhas, *smartcards* e certificados digitais, além da criptografia, *firewall*, etc.

Figura 17 - Diagrama das barreiras de segurança.



Fonte: Autoria Própria.

- **Discriminar:** Aqui o importante é se cercar de recursos que permitam identificar e gerir os acessos, definindo perfis e autorizando permissões. Os sistemas são largamente empregados para monitorar e estabelecer limites e acesso aos serviços de telefonia, perímetros físicos, aplicações de computador e bancos de dados. Os processos de avaliação e gestão do volume de usos dos recursos, como e-mail,

impressora, ou até mesmo o fluxo de acesso físico aos ambientes, são bons exemplos das atividades desta barreira.

- **Detectar:** Mais uma vez agindo de forma complementar às suas antecessoras, esta barreira deve munir a solução de segurança de dispositivos que sinalizam, alertam e instrumentam os gestores da segurança na detecção de situações de risco. Seja em uma tentativa de invasão, uma possível contaminação por vírus, o descumprimento da política de segurança da empresa, ou mesmo a cópia e envio de informações sigilosas. Entram aqui os sistemas de monitoramento e auditoria para auxiliar na identificação de atitudes de exposição, como o antivírus e os sistemas de detecção de intrusos, que reduzem o tempo de resposta a incidentes.
- **Deter:** Representa o objetivo de impedir que a ameaça atinja os ativos que suportam o negócio. O acionamento desta barreira, ativando seus mecanismos de controle, é um sinal de que as barreiras anteriores não foram suficientes para conter a ação da ameaça. Neste momento, medidas de detenção, como ações administrativas, punitivas e bloqueio de acessos físicos e lógicos, respectivamente a ambientes e sistemas, são bons exemplos.
- **Diagnosticar:** Apesar de representar a última barreira no diagrama, esta fase tem um sentido especial de representar a continuidade do processo de gestão de segurança. Pode parecer o fim, mas é o elo com a primeira barreira, criando um movimento cíclico e contínuo. Devido a esses fatores esta é a barreira de maior importância. Deve ser conduzida por atividades de análise de riscos que considerem tanto os aspectos tecnológicos quanto os físicos e humanos, sempre orientados às características e às necessidades específicas dos processos de negócio da empresa.

6.3.1. Controle de acesso

A expressão Controle de Acesso define um conjunto sistemicamente organizado de barreiras de proteção (física ou lógica), adotadas por uma empresa.

Tais barreiras têm um papel fundamental em uma organização, pois protegem os ativos organizacionais contra acessos indevidos, além de permitir acesso aos autênticos usuários desses ativos. Podemos definir acesso como um fluxo de informação que ocorre entre um sujeito e um objeto. Logo, o fluxo de informações numa organização é protegido pelo sistema de controle de acessos.

O termo controle de acesso é uma referência à prática de permitir o acesso a uma propriedade, prédio, ou sala, apenas para pessoas autorizadas e na segurança da informação, é composto dos processos de autenticação (identifica quem acessa o sistema), autorização (determina o que um usuário autenticado pode fazer) e auditoria (diz o que o usuário fez).

O controle físico de acesso pode ser obtido através de pessoas (um guarda, segurança ou recepcionista); através de meios mecânicos como fechaduras e chaves; ou através de outros meios tecnológicos, como sistemas baseados em cartões de acesso. Existem três tipos definidos de controle de acesso lógico: MAC (*Mandatory Access Control*), DAC (*Discretionary Access Control*) e RBAC (*Role Based Access Control*).

- **MAC** - Controles Baseados em Regras Gerais ou Obrigatórias: É usado para controlar acesso a arquivos ou recursos associando classificações para recursos do sistema e comparando isto ao nível de sensibilidade com que um usuário está operando. Com MAC, uma pessoa pode atribuir um nível de segurança a cada usuário e certificar-se de que todos os usuários têm somente o acesso aos dados de um isolamento.
- **DAC** - Controles Baseados em Identidade ou Discricionários: É usado para controlar acesso a arquivos ou recursos, colocando restrições no acesso do usuário aos recursos. O propósito principal é limitar o acesso de usuários a um arquivo. O dono do arquivo controla acessos ao arquivo por outros usuários.
- **RBAC** - Controles Baseados em Papéis: É um método de controlar acesso a um computador ou recursos de rede baseados nas funções de usuários individuais em uma empresa. Neste contexto, acesso é a habilidade de um usuário individual executar uma tarefa específica, como ler, criar ou modificar um arquivo. São definidas de acordo com a

competência, autoridade e responsabilidade de trabalho em uma empresa.

6.4. Políticas de *Backup*

Em informática, cópia de segurança (*backup*) é a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Atualmente muito se fala em *backup*, como também toda e qualquer empresa faz (ou tenta fazer) *backup* de seus dados. A metodologia e os conceitos sobre *backup* encontram-se dispersos em diversos livros que tratam de segurança da informação, além de inúmeros sites da Internet também abordarem tal tema.

Na eventualidade de ocorrência de um incidente, os dados devem ser repostos, recorrendo então à informação armazenada na cópia de segurança. A recuperação dos dados deverá ser efetuada rapidamente e de forma eficiente, para que os serviços não se encontrem inativos por muito tempo. A prioridade da reposição dos dados deve ser estabelecida, conforme as necessidades da organização.

A política de *backup* deve estabelecer quais as informações serão copiadas e de quanto em quanto tempo, quem será o responsável, seu local de armazenamento além do plano de recuperação de dados.

O plano de recuperação de desastres é composto por cenários e procedimentos para recuperação de ativos, quando ocorrer uma falha devido a alguma inconsistência ocorrida em virtude de ameaças como incêndio, enchente, vandalismo, sabotagem ou falhas de tecnologia.

O *backup* é uma das tarefas mais incômodas na administração de sistemas e deve ser nossa última linha de defesa contra a perda de dados, porém, se não pudermos restaurá-los não servirão para nada. Todas as mídias de *backup*s devem ser testadas periodicamente.

Existem diversas técnicas para realizar *backup* de dados e também diferentes tipos. O *backup* total (*Full*) faz a cópia de todos os arquivos e dados. O *backup* incremental só copia os arquivos e dados que foram alterados desde ó último

backup e é dividido em dois tipos. O incremental acumulado faz a cópia de todos os dados alterados desde o ultimo *backup full*. O incremental diferencial copia os dados alterados desde o ultimo *backup* diferencial.

Devemos nos lembrar de que as mídias de *backup* são alguns dos recursos mais valiosos de uma empresa, portanto, uma boa política de *backup* pode salvar a empresa caso ocorra um desastre.

6.5. Política de *Firewall*

A necessidade de atuação em rede, com comunicação distribuída, define a necessidade da interconexão entre as redes. Esta mesma interconexão que proporciona grande economia de recursos, agilidade em serviços e o aumento de conhecimentos, introduz novas ameaças. Por exemplo, a interconectividade permite a usuários não autorizados a possibilidade de acesso a informações sensíveis de praticamente, qualquer lugar do mundo. A primeira linha de defesa neste caso, geralmente é feita com o uso de um *firewall*.

Um *firewall* é um dispositivo estabelecido como uma barreira que deve ficar no perímetro de uma rede segura com outras redes, geralmente inseguras (normalmente ele liga a rede interna de uma organização à *internet*), protegendo a rede interna de ameaças externas, isolando estas redes e controlando o acesso aos dispositivos de rede.

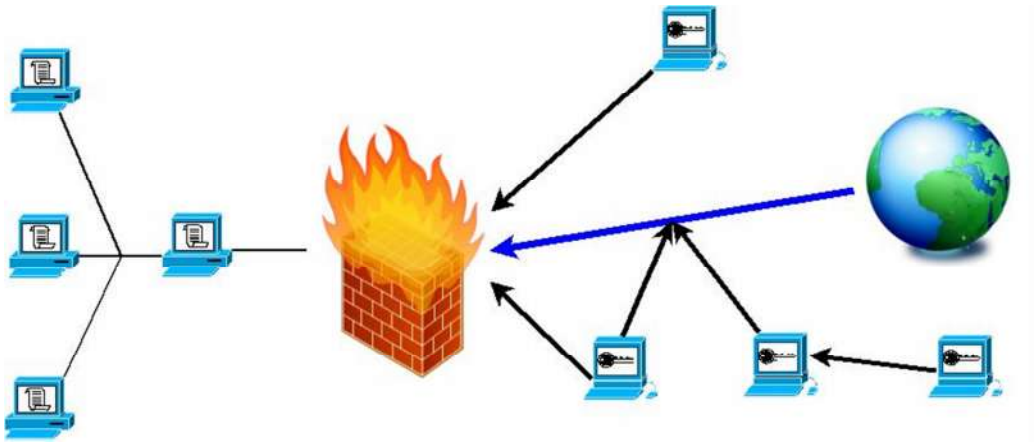
O propósito de um *firewall*, bem como o seu posicionamento no limiar entre redes, é forçar que todas as conexões passem através dele, de forma que as regras de filtragem possam atuar eficazmente durante uma tentativa de comunicação. Além da filtragem de pacotes, um *firewall* pode fornecer diversos tipos de serviços, como por exemplo, a Tradução de Endereços de Rede, conhecida por NAT (*Network Address Translation*), que é a tecnologia que permite que vários computadores compartilhem poucos (ou até mesmo apenas um) endereços de rede válidos na *Internet*.

Os *firewalls* podem ser divididos em duas grandes classes: filtros de pacote e servidores *proxy*:

- **Filtros de Pacotes:** A filtragem de pacotes é um dos principais mecanismos que, mediante regras definidas pelo administrador em um

firewall, permite ou não a passagem de datagramas IP em uma rede. Poderíamos filtrar pacotes para impedir o acesso a um serviço de Telnet, um chat ou mesmo um site na Internet. O modelo mais simples de *firewall* é conhecido como o *dual homed system*, ou seja, um sistema que interliga duas redes distintas. Este sistema possui um servidor com duas placas de rede que faz com que os usuários possam falar entre si. O exemplo clássico é um *firewall* entre uma Intranet e a *Internet*, como mostra a Figura 18.

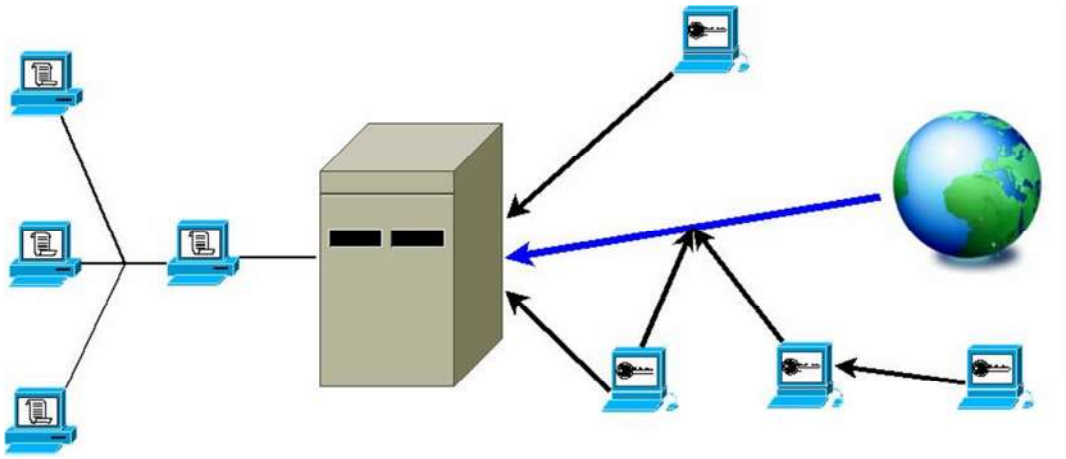
Figura 18 – Representação do Firewall.



Fonte: Autoria Própria.

- **Servidores *Proxy*:** Permite executar a conexão ou não a serviços em uma rede de modo indireto. Normalmente os *proxies* são utilizados como *caches* de conexão, ou seja, armazenam copias das páginas para serviços *Web*. Um *proxy* é utilizado em muitos casos como elemento de aceleração de conexão em *links* lentos, uma vez que as páginas já estão armazenadas nesse servidor, como ilustra a Figura 19.

Figura 19 – Representação do Servidor de Proxy.



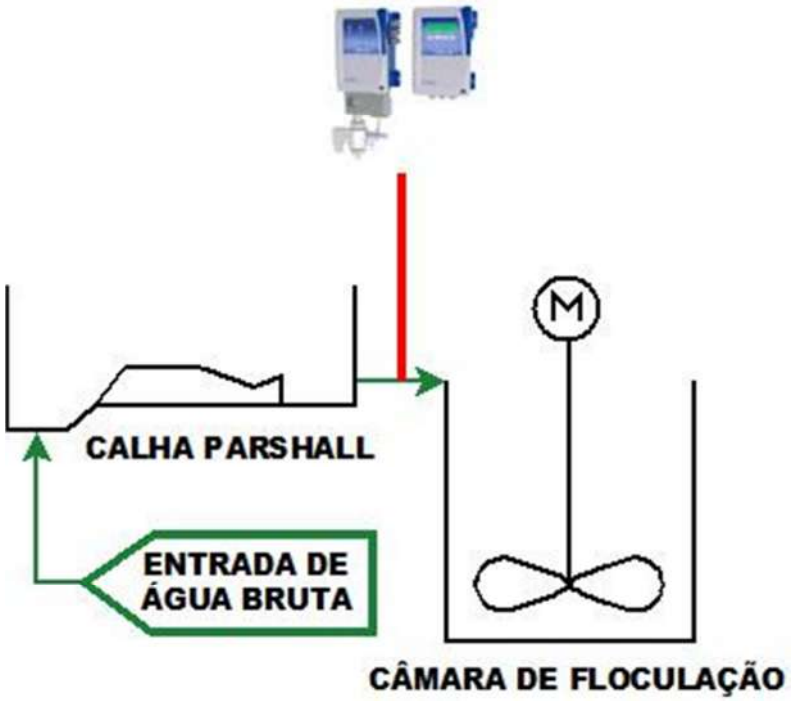
Fonte: Autoria Própria.

7. UNINDO A TRÍADE TRATAMENTO, AUTOMAÇÃO E SEGURANÇA.

Para que haja a automação do sistema de tratamento de água com efetiva segurança, há de se instalar os instrumentos inteligentes, interligando-os ao sistema supervisório para que o mesmo tome as decisões pertinentes em cada etapa do processo.

O primeiro passo neste caso específico é a instalação do monitor de coagulação. A aplicação deste equipamento fará um rigoroso controle da dosagem do coagulante, visto que ele trabalha com a medição de diferença de cargas elétricas. Portanto, não mais serão de suma importância as variáveis vazão e turbidez descritas como fundamentais em capitulo anterior. Isto trará a garantia de controle da dosagem do coagulante, aplicando a quantidade exata de produto químico, evitando o desperdício e trazendo segurança e economia na operação da ETA. A instalação deste equipamento faz-se necessária em um ponto após a total dispersão do coagulante na água bruta, no caso, a entrada dos tanques de floculação, como mostra a Figura 20.

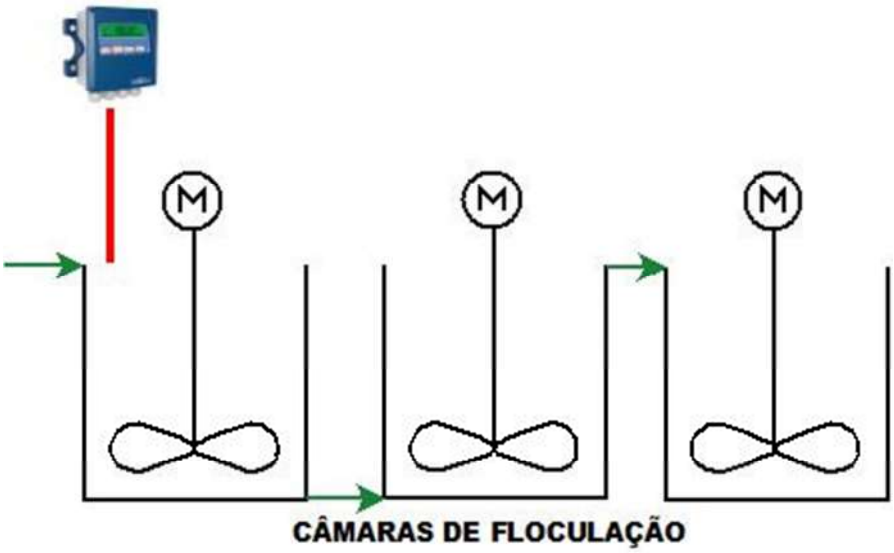
Figura 20 - Ponto de instalação do monitor de coagulação.



Fonte: Autoria Própria.

Em seguida, para o monitoramento do pH ideal de coagulação, faz-se necessária a instalação de um pHmetro inteligente, que controla a bomba de dosagem de alcalinizante, informando ao sistema o pH atual de coagulação e podendo o mesmo realizar a correção se necessário, com aumento, ou diminuição da dosagem do alcalinizante. O ponto ideal para a instalação de tal equipamento, é a primeira câmara de floculação, como indicado na Figura 21.

Figura 21 - Ponto de instalação do pHmetro de controle da coagulação.



Fonte: Autoria Própria.

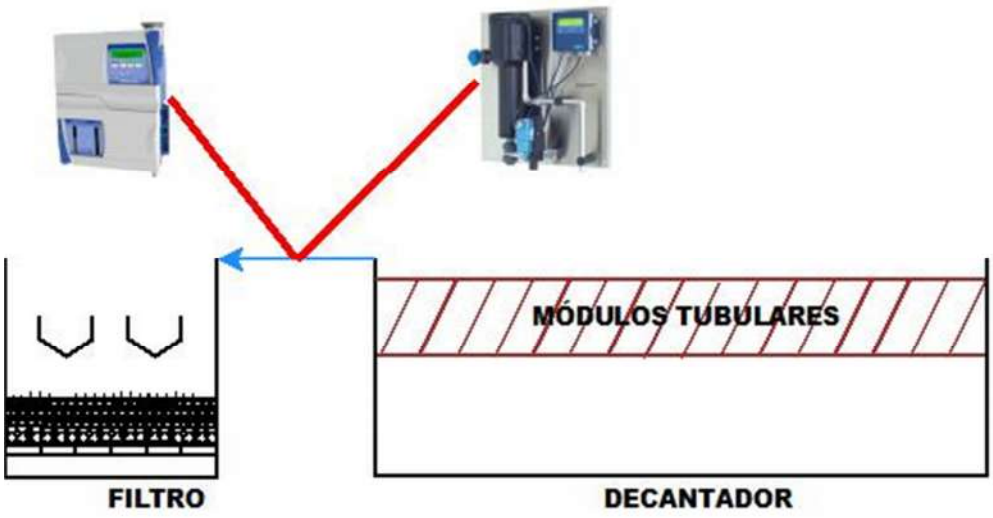
Figura 22 - Ponto de instalação do medidor de vazão.

Fonte: Autoria Própria.

O gradiente de velocidade de agitação dos floculadores é a próxima peça deste quebra-cabeça. Enviando o sinal do medidor de vazão, instalado no ponto indicado pela Figura 22, ao sistema supervisório, o mesmo pode efetuar o cálculo do gradiente efetivo necessário aos agitadores, controlando a velocidade de agitação através dos inversores de frequência, otimizando a floculação e consequentemente as etapas seguintes do tratamento.

A seguir, a automação com segurança do sistema de tratamento necessita do controle da turbidez e cor de saída do decantador, e que atualmente não é feito nesta ETA. A instalação de tais equipamentos visa à segurança dos controles efetivados anteriormente, informando ao sistema possíveis falhas dos instrumentos anteriores. A Figura 23 mostra o local para instalação destes equipamentos.

Figura 23 - Ponto de instalação dos analisadores de cor e turbidez.

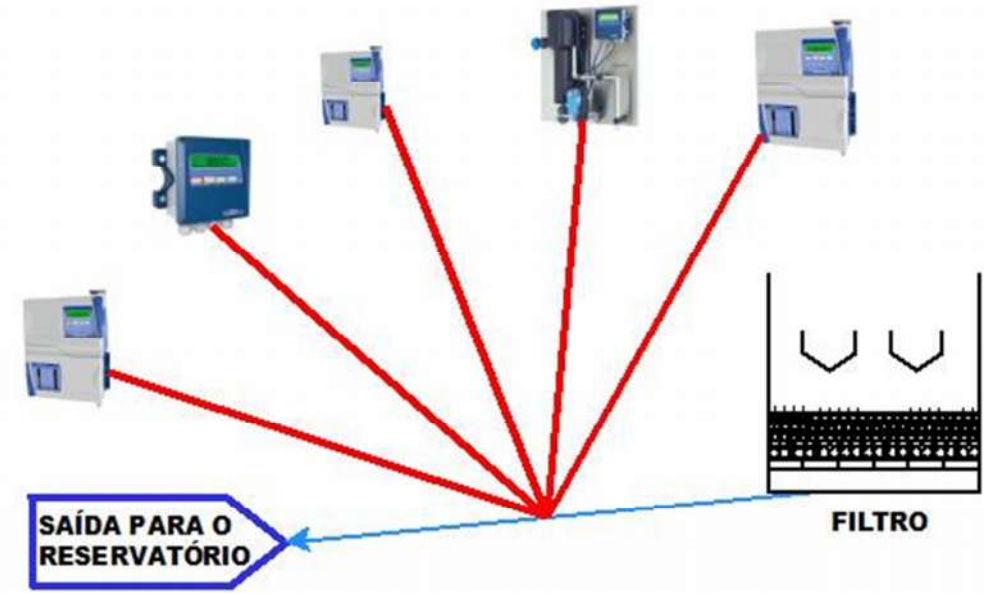


Fonte: Autoria Própria.

Após a filtração faz se necessária à instalação do turbidimetro inteligente e, cada filtro deve possuir seu próprio turbidimetro, para a otimização dos resultados obtidos. Para que haja um controle automático de lavagem de filtro também é necessária a instalação de sensores de nível em cada filtro. Uma alternativa mais econômica, mas não indicada, é a instalação de apenas um turbidimetro para a saída geral da ETA. Porém, o controle seguro e efetivo da qualidade da água deverá possuir ao menos um turbidimetro em cada saída de filtro.

Após a saída de água dos filtros, os equipamentos necessários são os seguintes: turbidimetro, analisador de cor, controlador de pH, analisador de cloro e analisador de flúor, como indicado na Figura 24.

Figura 24 - Ponto de instalação dos analisadores da água tratada.



Fonte: Autoria Própria.

Utilizando a arquitetura de redes em barramento, podemos fazer com que todos os equipamentos trabalharem em conjunto, pois estando estes ligados ao mesmo conjunto de cabos, formam então uma rede de campo. O mercado moderno oferece variedade de instrumentação inteligente com saída RS485, o protocolo ponto/multiponto ideal para a ligação dos instrumentos na rede de campo idealizada neste projeto, que por sua vez, serão interligados através de um CLP ao sistema supervisório de controle da estação de tratamento. Uma vez que todos os equipamentos citados estejam devidamente instalados e em funcionamento, a ETA pode ser considerada automatizada.

Logo após a automação do sistema, e logo que as informações estiverem chegando e sendo tratadas pelo software de controle, o próximo passo é atrelar estas informações a um banco de dados, situado em um servidor próprio, já existente nesta autarquia. Após a confecção de uma página dentro do site do próprio DAE, tais informações podem ser acessadas por qualquer pessoa conectada à rede mundial de computadores, a internet.

De acordo com a ISO/IEC 27001, “O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas.”.

Para proporcionar o funcionamento seguro e ininterrupto deste sistema, a confecção de uma PSI deve seguir as orientações contidas na ISO/IEC 27002. Esta ISO nos trás em seu item “4 Análise/avaliação e tratamento de riscos**”**, o primeiro argumento efetivo para a confecção desta PSI, onde os riscos devem ser identificados, quantificados e priorizados para que os resultados determinem as ações e os controles a serem implementados. A norma ainda indica que este processo de avaliação deva ser realizado várias vezes, afim de que todas as partes da organização sejam cobertas. Portanto, a correta seleção dos controles adequados norteará a confecção de tal PSI.

A redundância de equipamentos nos trás uma excelente forma de assegurar que as informações medidas cheguem ao seu destino final. Desta maneira, para cada equipamento citado ao decorrer deste trabalho, outro do mesmo modelo pode ser adicionado, operando em modo de espera (*stand-by*).

No quesito barreiras de segurança, a ETA apresenta algumas câmeras de vigilância, porém, devido à distribuição e localização, as mesmas são ineficientes a uma efetiva segurança das informações. Outras barreiras de segurança físicas, como catracas de acesso, vigias, e grades devem ser implementados por todo o perímetro na elaboração da PSI. As barreiras de segurança lógica também devem ser revistas, pois o sistema supervisório instalado no computador da ETA permite a autenticação individual de quem acessa o sistema, podendo suas permissões serem configuradas pelo administrador e com geração de logs de acesso para futura auditoria.

Logicamente, a PSI deve contemplar ainda uma política de *backup*, podendo o DAE recorrer às informações armazenadas em cópia de segurança na eventualidade de ocorrência de um incidente. Tendo em vista a distância entre a ETA e a sede administrativa da autarquia, a sugestão de armazenamento de uma cópia em cada local reduziria os riscos para um nível aceitável.

Para complementação da segurança deste projeto, a revisão da politica de *firewall* já existente protegerá os dados contidos nos servidores desta autarquia, evitando o acesso indesejado às informações tão importantes e vitais ao perfeito e seguro sistema de tratamento do DAE de Santa Bárbara d’Oeste.

8. CONSIDERAÇÕES FINAIS

Analisando a evolução da humanidade constatamos que a cada minuto que deixamos para trás, uma nova informação nos é apresentada. Essas novas informações quando agrupadas nos levam a novas técnicas, ocasionando o lançamento de dispositivos cada vez mais modernos. Estas tecnologias embarcadas ao longo de nossa existência produzem equipamentos capazes de gerir automaticamente qualquer tipo de processo.

A água é nosso bem mais precioso e, para podermos utilizá-la, devemos lançar mão de toda tecnologia disponível em seu tratamento. Como apresentado neste trabalho, a maioria das estações de tratamento no Brasil possuem todos os seus controles dependendo das mãos humanas, e qualquer mínimo erro de operação pode acarretar altos custos, ou pior, comprometer a saúde de quem consumir esta água, gerando outros diversos desperdícios de recursos.

Atrelando os fatos citados, podemos concluir que a excelência em controle de processos ocasionada pela aplicação de tecnologias pode reduzir inúmeros tipos de custos, aperfeiçoar a segurança das informações obtidas e elevar a qualidade do produto final. Para que haja tais aperfeiçoamentos e economia, nossas estações de tratamento de água devem caminhar ao encontro da tecnologia, ou seja, a **automação como fonte de segurança das informações**.

A automação consiste em conexão de tecnologias, e esta mesma interconexão que proporciona grande economia de recursos e agilidade em serviços nos introduz novas ameaças, que provêm de diferentes tipos de fontes como fenômenos naturais e ações humanas (propositais ou não), e para obter proteção contra tais ameaças é necessária a implementação de controles que devem ser selecionados e aplicados para assegurar que os riscos sejam reduzidos a um nível aceitável pela organização.

A partir dos assuntos explanados neste trabalho, destaca-se a importância da tecnologia como fator de aperfeiçoamento em sistemas de tratamento de água, trazendo segurança e controle na operação das estações, minimizando as probabilidades de falha e desbaratamento de insumos, ocasionando a homogeneidade do produto final e a segurança das informações geradas pelo sistema.

Fundamentado no que diz Mascarenhas (2005, p. 3) “O país não poderá manter um crescimento econômico sustentado, a menos que expanda o volume e melhore a qualidade dos investimentos em infra-estrutura (sic).”, podemos efetuar uma análise ao nosso redor, constatando que o nível de saneamento básico apresentado em nosso país está muito abaixo das necessidades de nossa população. Como parte mais importante da infraestrutura de saneamento básico, as estações brasileiras de tratamento de água na maioria dos casos, também deixam de receber os investimentos necessários para manterem-se em condições razoáveis de operação.

O investimento em educação é primordial para o avanço em tecnologias, que quando aplicadas em pontos estratégicos, como o saneamento básico, garantem economia de recursos em diversos outros setores, como exemplo: a saúde. Ou seja, uma estação de tratamento de água automatizada garante a capitalização tanto para a autarquia quanto para a união, assegurando ainda a qualidade do produto final e também a saúde de quem consome a água.

Os recursos economizados no tratamento de água podem ser aplicados tanto na própria ETA quanto em outros setores da própria autarquia, como exemplo a aquisição de outras tecnologias e equipamentos modernos para o tratamento de efluentes, manutenções preventivas e corretivas, programas educacionais, controle e combate ao desperdício de água, e outros investimentos em melhorias para a distribuição deste bem que nos é vital.

As conclusões que se chegam com este trabalho é que a automação pode perfeitamente ser utilizada como fonte de segurança das informações e inclusive das estações de tratamento de água em si, além da economia para investimentos em outros setores e ainda o cumprimento do objetivo do DAE: “tornar-se referência em serviços de água e saneamento, buscando sempre a excelência.”, além de cumprir com todos objetivos do próprio trabalho e com um propósito pessoal: “**Assegurar que a informação derivada da automação do processo de tratamento de água, possa servir como fonte de conhecimento para a inovação tecnológica na área e melhoria contínua do saneamento básico brasileiro**”.

REFERÊNCIAS BIBLIOGRÁFICAS

ACHON, C. L. **Ecoeficiência de Sistemas de Tratamento de Água a Luz dos Conceito da IS0 14.001.** Dissertação de doutorado USP – 2008.

ALVES, A. R**. Política de Segurança da Informação: Análise ergonômica da difusão das normas em uma organização pública e seu impacto nos comportamentos inseguros.** Brasília: O autor, 2011. 61 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (Brasil). **NBR 12216/1992: Projeto de estação de tratamento de água para abastecimento público**. Rio de Janeiro, 1992. Disponível em: http://www.ebah.com.br/content/ABAAABiI0AH/nbr-12216-1992-projeto-estacao-tratamento-agua-abastecimento-publico. Acesso em: 02 abr. 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: Tecnologia da Informação - Técnicas de Segurança - Código de prática para a gestão da segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2006. 34p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: Tecnologia da Informação - Técnicas de Segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005. 120p.

BOTERO, W. G. **CARACTERIZAÇÃO DE LODO GERADO EM ESTAÇÕES DE TRATAMENTO DE ÁGUA: PERSPECTIVAS DE APLICAÇÃO AGRÍCOLA.** Quim. Nova, Vol. 32, No. 8, 2018-2022, 2009.

BRASIL. Ministério da Saúde. **Portaria 2914**. Dispõe sobre os procedimentos de controle e de vigilância da qualidade da água para consumo humano e seu padrão de potabilidade. Brasília, DF: Ministério da Saúde, dez. 2011.

BARRETO, A. A. **A QUESTÃO DA INFORMAÇÃO**. 1994. Disponível em: https://bibliotextos.files.wordpress.com/2012/03/a-questao-da-informac3a7c3a3o.pdf Acesso em: 09 abr.. 2015.

BARRETO, A. S. **Controle de acesso lógico: um estudo sobre o caso da TI na Faculdade UnB Gama.** Brasília: O autor, 2012. 69 p.

CAPANEMA, S. P. **Instrumentação e controle de uma estação de tratamento de água.** Dissertação de Mestrado. UFMG – 2004.

CEPIK, M. A. C. **Espionagem e Democracia.** Fundação Getúlio Vargas, 2003. Disponível em: http://books.google.com.br/books?id=xERuDARa8wC&printsec=frontcover. Acesso em: 20 abr. 2015.

COSTA, E. K. **Gestão de Configuração de Firewalls no Banco do Brasil: Racionalização das bases de regras no ambiente Extranet sob a ótica do ITILv2.** Brasília: O autor, 2011. 110 p.

DI BERNARDO, L. **Métodos e Técnicas de Tratamento de Água**. Rio de Janeiro, ABES, V.1, 1993.

DIGIMED INSTRUMENTAÇÃO ANALÍTICA. Disponível em: <http://www.digimed.ind.br/br/>. Acesso em 25 mai. 2015.

DOS ANJOS, E. M. **Perfil Profissional de Curso de Especialização em Defesa Cibernética para Integrantes do Exército Brasileiro: uma Proposta com Base no Ensino por Competência.** Brasília: O autor, 2011. 63 p.

FERNANDES, J. H. C. **SISTEMAS, INFORMAÇÃO & COMUNICAÇÃO** 2011. 51p. Disponível em http://www.cic.unb.br/~jhcf/. Acesso em 31 mar. 2015.

FERREIRA, A. B. H. **Novo Dicionário da Língua Portuguesa.** 2.ed. Editora Nova Fronteira – Rio de Janeiro – 1996. Disponível em: <https://books.google.com.br/books?id=hVhGAgAAQBAJ&pg=PA146&lpg=PA146&dq=FERREIRA,+Aur%C3%A9lio+Buarque+de+Holanda,+Novo+Dicion%C3%A1rio+da+L%C3%ADngua+Portuguesa,+2%C2%AA+edi%C3%A7%C3%A3o+revista+e+aumentada,+Editora+Nova+Fronteira&source=bl&ots=cld5BVGDLZ&sig=e_qfgGGZNzpDAfVnTTiaqa6f2oo&hl=pt-BR&sa=X&ei=jNprVaCPKYudNuODgZgK&ved=0CB0Q6AEwAA#v=onepage&q=automa%C3%A7%C3%A3o&f=false>. Acessado em: 02 abr. 2015.

FONSECA, F. R. **Modelo para automação de sistemas de tratamento de água.** Dissertação de Mestrado. EP-USP – 2009. 128p.

HELLER, L.; PÁDUA, V. L. **Abastecimento de água para consumo humano.** 2.ed. Minas Gerais: UFMG, 2010. Disponível em: http://pt.scribd.com/doc/166329229/Abastecimento-de-agua-para-consumo-humano-volume-2-pdf#scribd. Acessado em: 31 mar. 2015.

HOUAISS - **Dicionário online**. Disponível em : <http://houaiss.uol.com.br/>. Último acesso em: 07 abr. 2015.

JESUS, F. S. **Organização de sistemas de rede: um estudo de caso sob a ótica de prevenção à ataques cibernéticos.** Brasília: O autor, 2011. 68 p.

LIBÂNIO, M. **Fundamentos da qualidade e tratamento de água**. 2.ed. Campinas, SP. Átomo. 2008 441p.

MACEDO, J. A. B. **Águas & Águas**. 3. ed. Minas Gerais: CRQ – MG, 2007.

MARTINS, A. P. C. **Avaliação dos Controles de Acessos Lógicos Adotados em uma Organização Pública sob a Ótica das Normas ABNT NBR ISO/IEC 27002:2005 e NC 07/IN01/DSIC/GSIPR.** Brasília: O autor, 2011. 125 p.

MASCARENHAS, F. J. **A Infra-Estrutura no Brasil**, Conselho de Infra- Estrutura, Brasília, 2005.
NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec, 2007.

PAVANELLI, G. **Eficiência de diferentes tipos de coagulantes na coagulação, floculação e sedimentação de água com cor ou turbidez elevada.** São Carlos, SP. 215p. (Dissertação Mestrado) – Universidade de São Paulo, 2001.

PEREIRA, S. L. **Aspectos Sobre Processos Automatizados de Pesagem Rodoferroviária: Uma Proposta de Modernização de Postos em Operação**, tese (doutorado), EP-USP, 1995.

PIOVESAN, A. S. **Instrumentação Inteligente: Implementação de Malha de Controle no Nível dos Instrumentos de Processo**. São Paulo, 1993. Dissertação (Mestrado) - Escola Politécnica, Universidade de São Paulo.

REZENDE, D. A.; ABREU A. F. **Tecnologia da informação**. São Paulo: Atlas. 2000.

RIBEIRO, A. J. **Gestão de segurança em redes sem fio: A proteção do padrão IEEE 802.11 na Administração Pública Federal.** Brasília: O autor, 2011. 78 p.

ROBREDO, J. **Da Ciência da Informação aos Sistemas Humanos de Informação**. Brasília: Thesauros. 2005.

SIMIÃO, R. S. **Segurança da Informação e Comunicações: conceito aplicável em organizações governamentais.** Brasília: O autor, 2009.

SOUSA, F. V. S. **Segurança das Informações Públicas: Segurança Cibernética / Fábio Vinícius Santos Sousa.** Brasília: O autor, 2011. 33 p.

SILVEIRA, P. R. & SANTOS, W. E. **Automação e Controle Discreto**. São Paulo: Érica, 1998, p.20-24.

SIMON, I. **A ARPANET**, 1997. Disponível em: <http://www.ime.usp.br/~is/abc/abc/node20.html>. Acesso em: 02 abr. 2015.

SOUZA, M. **Proposta de um sistema de gestão empregando instrumentação inteligente e redes de campo na automação do processo de tratamento de água.** Dissertação de Mestrado. USP - 2006. 161 p.

TSUTIYA. M. T. **Abastecimento de Água.** São Paulo – SP. Departamento de Engenharia Hidráulica e Sanitária da Escola Politécnica da Universidade de São Paulo. 2004. 643 p.

VENEZIANO, W. H. **ORGANIZAÇÕES E SISTEMAS DE INFORMAÇÃO**. 13p. Disponível em: <http://www.cic.unb.br/~jhcf/MyBooks/cegsic/2009_2011/05_D5-TextoBase.pdf>. Acesso em: 01 abr. 2015.