ISSN- 2966-0785 REVISTA ACADÊMICA DA LUSOFONIA

SISTEMAS INTEGRADOS DE CONTROLE DE PORTARIA EM PLANTAS INDUSTRIAIS: UM ESTUDO BIBLIOGRÁFICO

Kelly Rodrigues Marcolino[1]
Iveltyma Roosemalen Passos Ibiapina[2]

RESUMO
O presente estudo tem como tema a contribuição dos sistemas integrados de controle de portaria para a segurança e a eficiência em plantas industriais. A crescente complexidade dos ambientes de produção exige soluções robustas para a gestão de acessos, visando mitigar riscos e otimizar processos. O objetivo deste artigo é analisar a literatura existente sobre o tema, explorando os conceitos, tecnologias e benefícios associados à implementação desses sistemas. A metodologia empregada é a pesquisa bibliográfica, baseada em obras clássicas e contemporâneas da área de segurança, automação e gestão industrial, bem como artigos científicos e normas técnicas. Espera-se com este trabalho demonstrar como a integração de tecnologias como controle de acesso biométrico, CFTV e softwares de monitoramento pode aprimorar a segurança patrimonial, a proteção de dados e a eficiência operacional, oferecendo uma contribuição relevante para a gestão estratégica de indústrias que buscam modernizar seus processos.

Palavras-chave: Portaria, Plantas industriais, Sistemas Integrados, Segurança, Automação.

[1]Discente do Curso Superior de Tecnologia em Gestão Comercial do Instituto Federal de Rondônia (IFRO), Campus Jaru. E-mail:kellyrodrigues.krm@gmail.com
[2] Doutor em Administração e Professor do Instituto Federal de Rondônia, Campus Jaru. E-mail: iveltyma.ibiapina@ifro.edu.br

ISSN- 2966-0785 REVISTA ACADÊMICA DA LUSOFONIA

1.INTRODUÇÃO

A segurança e o controle de acesso são componentes cruciais para a operação bem-sucedida de qualquer ambiente, mas adquirem uma importância ainda maior em plantas industriais. Nestes locais, a movimentação de pessoas, veículos e cargas é intensa e, muitas vezes, envolve o manuseio de materiais sensíveis, equipamentos de alto valor e informações estratégicas (SILVA, 2019).

A falta de um controle rigoroso pode levar a incidentes de segurança, perdas financeiras, interrupção da produção e riscos à integridade física dos colaboradores. A relevância desse tema é corroborada por Fischer (2007), que afirma que a segurança em ambientes fabris é um sistema complexo que engloba a proteção de bens, pessoas e processos.

O problema de pesquisa deste estudo reside em compreender de que maneira os sistemas de portaria, quando integrados, contribuem para a melhoria da segurança e eficiência nesses ambientes. Em um cenário onde a automação e a tecnologia se tornam onipresentes, as portarias tradicionais, baseadas em controle manual, se mostram ineficientes e vulneráveis, impactando negativamente a produtividade e a gestão de riscos (MACHADO, 2020).

Nesse sentido, o objetivo geral deste trabalho é analisar a literatura existente sobre o controle de portarias, explorando os conceitos, tecnologias e benefícios associados à implementação desses sistemas. Para atingir tal objetivo, foram conceituados e caracterizados os elementos de uma planta industrial e seus desafios de segurança, além deidentificar as tecnologias que compõem os sistemas integrados de controle de acesso e, por fim,discutir sobre os benefícios e as limitações da implementação desses sistemas.

A justificativa para esta pesquisa é a crescente necessidade de otimização dos processos de segurança. Em um cenário onde a automação e a tecnologia se tornam onipresentes, as portarias tradicionais, baseadas em controle manual, se mostram ineficientes e vulneráveis. Este estudo oferece uma base teórica para gestores e profissionais da área, justificando o investimento em soluções tecnológicas que promovem um ambiente de trabalho mais seguro e produtivo.

O artigo está estruturado em seis seções, incluindo a presente introdução, seguidas pelo referencial teórico onde é apresentada a base teórica do estudo, métodos onde é explicado quais foram os procedimentos utilizados, resultados e discussão dos estudos encontrados na área, considerações finais onde são tecidas discussões e confrontos dos resultados e, por fim, as referências.

2. REFERENCIAL TEÓRICO

2.1. Plantas industriais: conceitos e características

Uma **planta** industrial é um complexo multifuncional, um ecossistema operacional que vai além de meros edifícios e maquinários. A sua principal característica é a concentração de recursos críticos, incluindo matéria-prima, capital intelectual e tecnologia de ponta, tudo com o propósito de transformar insumos em produtos acabados (Fischer, 2007). Em sua essência, o ambiente industrial moderno é um espaço de alta complexidade, onde a segurança e a produtividade estão diretamente interligadas. A proteção de ativos, sejam eles físicos ou intelectuais, é uma prioridade, pois falhas de segurança podem resultar em perdas financeiras catastróficas e na interrupção de cadeias de suprimentos globais.

A diversidade de operações dentro de uma planta industrial demanda soluções de segurança flexíveis e escaláveis. Uma fábrica de alimentos, por exemplo, possui desafios de controle de acesso diferentes de uma siderúrgica ou de uma usina petroquímica, onde os riscos de acidentes são significativamente maiores (Silva, 2019). Essa complexidade operacional exige que os sistemas de segurança sejam modulares e possam ser configurados para atender às necessidades específicas de cada setor, desde áreas de armazenamento de insumos até laboratórios de pesquisa e desenvolvimento. A gestão do fluxo de pessoas e veículos é um elemento central para garantir que apenas indivíduos autorizados e devidamente preparados acessem áreas de risco.

Além da diversidade interna, as plantas industriais são pontos-chave na logística global, recebendo e despachando um fluxo contínuo de veículos, caminhões e contêineres. O controle de acesso veicular é, portanto, tão vital quanto o de pessoas. Um sistema de portaria ineficiente pode gerar longas filas, atrasos na entrega e aumento nos custos operacionais, comprometendo a competitividade da empresa no mercado (Moraes, 2015). A otimização desse processo é um dos principais motivadores para a adoção de tecnologias avançadas, como o uso de RFID para identificação automática de veículos.

A segurança em ambientes industriais não se restringe apenas à proteção contra ameaças externas, como roubos ou vandalismo. O controle interno é igualmente crucial. O acesso a equipamentos de alto valor, a documentos confidenciais ou a áreas de produção sensíveis deve ser rigorosamente controlado para evitar desvios, sabotagens ou apropriação indevida de informações proprietárias (Machado, 2020). Um sistema de portaria integrado,

que registra e monitora cada movimento, atua como uma ferramenta de auditoria e compliance, garantindo que as políticas de segurança da empresa sejam seguidas por todos.

A transformação digital tem alterado profundamente a natureza das plantas industriais, que agora estão repletas de sensores IoT (Internet das Coisas) e sistemas de automação interconectados. Esse ambiente "inteligente" exige que a segurança da portaria também seja inteligente, capaz de se comunicar com outros sistemas da planta, como o controle de estoque ou a gestão de produção (Souza, 2022). A portaria, que antes era uma barreira física, se transforma em um nó central de uma rede de segurança digital, capaz de tomar decisões baseadas em dados em tempo real.

2.2. Segurança em ambientes industriais

A segurança em ambientes industriais é um conceito multidimensional, que se estende para além da simples vigilância. Ela engloba a proteção patrimonial, a segurança dos dados e informações confidenciais, e a integridade física dos colaboradores (Silva, 2019). Os riscos são variados e complexos, incluindo desde eventos de baixo impacto, como o acesso não autorizado de um visitante a uma área restrita, até cenários de alta gravidade, como sabotagem, incêndios ou vazamentos de produtos químicos. A norma ISO 45001 sobre sistemas de gestão de segurança e saúde ocupacional, por exemplo, destaca a importância da prevenção e do controle de riscos no ambiente de trabalho.

A vulnerabilidade de uma planta industrial é determinada pela combinação de seus ativos de valor e a facilidade com que um agressor pode acessá-los. Uma portaria manual, por exemplo, é vulnerável à falha humana, como a distração do vigilante ou a falsificação de um crachá de identificação. Pereira (2018) aponta que a ausência de um sistema de controle de acesso robusto é uma das principais brechas de segurança em empresas de médio e grande porte. A falta de registro digital impede a rastreabilidade do histórico de acesso, dificultando a investigação de incidentes.

O controle de acesso em ambientes industriais é particularmente desafiador devido à diversidade de pessoas que transitam no local. Além dos funcionários fixos, há visitantes, prestadores de serviço, caminhoneiros, e até mesmo inspetores de órgãos reguladores. Cada grupo possui um nível de permissão de acesso diferente, o que exige um sistema flexível e hierárquico (Moraes, 2015). Um software de gestão de portaria eficiente permite a criação de perfis de acesso personalizados, garantindo que um prestador de serviço tenha permissão apenas para a área e o tempo necessários para realizar sua tarefa.

Além disso, a segurança industrial está intimamente ligada à segurança da informação. A entrada de dispositivos eletrônicos, como laptops e pen drives, pode representar uma ameaça de vazamento de dados ou de infecção por malware (Nogueira, 2021). Um sistema de portaria integrado pode incluir políticas que restringem a entrada de certos dispositivos ou que exigem um protocolo de verificação antes de permitir o acesso. Essa abordagem holística da segurança, que combina a proteção física e digital, é cada vez mais relevante no cenário da Indústria 4.0.

A resposta a emergências é outro pilar da segurança industrial. Em caso de incêndio, vazamento de gás ou qualquer outro evento de risco, é fundamental saber a localização exata de cada pessoa dentro da planta. Os sistemas de controle de acesso integrados fornecem essa informação em tempo real, facilitando a evacuação e o resgate. Essa capacidade de monitoramento em tempo real é vital para a conformidade com normas como a NR-23, que trata de proteção contra incêndios, e a ISO 14001, que aborda a gestão ambiental, garantindo que as ações emergenciais sejam rápidas e eficazes.

2.3. Portarias em sistemas industriais

As portarias, em seu formato tradicional, funcionam como barreiras primárias de controle. Elas são responsáveis por fiscalizar a entrada e saída de pessoas e veículos, registrando a visita em livros de papel ou planilhas simples (Moraes, 2015). Embora essa abordagem tenha sido a norma por décadas, ela apresenta sérias limitações. O registro manual é lento, suscetível a erros de digitação e ineficaz para auditar grandes volumes de dados. A falta de integração com outras áreas da empresa faz com que a portaria opere de forma isolada, sem informações em tempo real sobre a situação interna da planta.

A evolução tecnológica trouxe consigo a automação da portaria, transformando-a de um ponto de controle manual para um centro de gestão inteligente. A adoção de tecnologias como cartões magnéticos e leitores de código de barras foi um passo inicial nessa transição, acelerando o processo de registro e permitindo uma forma básica de rastreabilidade (Machado, 2020). No entanto, essas tecnologias ainda eram suscetíveis a fraudes, como o uso de credenciais de terceiros, o que abriu caminho para a necessidade de soluções mais seguras, como a biometria.

A portaria moderna é um ponto de entrada para o ecossistema de segurança da planta. A sua eficácia não reside apenas em impedir o acesso de pessoas não autorizadas, mas em gerenciar o fluxo de forma inteligente. Isso envolve a utilização de catracas eletrônicas para

controlar o acesso de pedestres e cancelas automáticas para veículos, tudo interligado a um software central. A norma ISO/IEC 27001, embora voltada para a segurança da informação, ressalta a importância do controle de acesso físico como parte de um sistema de gestão de segurança abrangente, reforçando que a proteção de dados começa na porta de entrada da empresa.

A função da portaria também se expande para o monitoramento de atividades internas. Através da integração com sistemas de CFTV, os operadores podem verificar a autenticidade de um acesso e monitorar o comportamento de pessoas e veículos em áreas críticas (Pereira, 2018). Essa vigilância proativa não apenas dissuade ações maliciosas, mas também permite uma resposta rápida a incidentes. Em caso de um evento suspeito, as câmeras podem ser direcionadas para a área, e a equipe de segurança pode ser acionada em segundos.

A portaria, em sua forma mais avançada, utiliza a tecnologia para criar um ambiente de segurança preditiva. Sensores no local podem coletar dados sobre o fluxo de pessoas, a frequência de acessos e os horários de pico. Esses dados, quando analisados por softwares de inteligência artificial, podem identificar padrões de comportamento incomuns ou anomalias que possam indicar uma ameaça potencial (Souza, 2022). A portaria, nesse contexto, deixa de ser reativa e se torna proativa, capaz de antecipar riscos e atuar preventivamente, o que é um diferencial competitivo no mercado.

Nesse sentido, os sistemas integrados de controle representam a evolução da segurança física. Conforme Machado (2020), a integração de tecnologias como CFTV (Circuito Fechado de Televisão), biometria (impressão digital, reconhecimento facial), RFID (Identificação por Rádio Frequência) e softwares de gerenciamento permite que a portaria opere de forma automatizada e inteligente. A informação coletada por cada tecnologia é centralizada e processada, permitindo uma visão holística e em tempo real do ambiente.

- CFTV e Análise de Vídeo Inteligente: Além da gravação, câmeras modernas utilizam análise de vídeo inteligente para identificar comportamentos suspeitos, detectar objetos esquecidos ou identificar intrusos em áreas restritas.
- Controle de Acesso Biométrico e Credenciais: A biometria oferece um nível de segurança superior, pois a credencial (impressão digital, face) não pode ser facilmente roubada ou emprestada. Sistemas de credenciais RFID (cartões de proximidade) permitem um acesso rápido e rastreável, e podem ser integrados a sistemas de controle de ponto.

- Softwares de Gestão de Segurança: A espinha dorsal do sistema integrado é o software de gestão. Ele centraliza as informações de todas as tecnologias (câmeras, catracas, sensores) em uma única interface, permitindo que os operadores monitorem o status de cada acesso, gerem relatórios detalhados e programem regras de acesso específicas para cada área e pessoa.

A implementação de sistemas integrados de controle de portaria traz uma série de benefícios. A eficiência operacional aumenta com a automação de processos, reduzindo o tempo de espera e otimizando a movimentação de pessoas. A redução de riscos é um dos principais ganhos, pois a tecnologia minimiza a vulnerabilidade a falhas humanas e permite uma resposta mais rápida a eventos de segurança.

Por fim, a tomada de decisão baseada em dados é aprimorada, uma vez que o software de gestão gera relatórios e análises sobre o fluxo de pessoas e incidentes, oferecendo informações valiosas para a gestão (SOUZA, 2022). O sistema pode, por exemplo, identificar picos de acesso em determinados horários, permitindo o dimensionamento mais adequado da equipe de segurança.

Apesar dos benefícios, a implementação desses sistemas não é isenta de desafios. Os custos iniciais de aquisição e instalação são, muitas vezes, elevados, o que pode ser uma barreira para pequenas e médias empresas. O treinamento de pessoal é fundamental para que os colaboradores operem o sistema de forma eficaz e compreendam sua importância para a segurança. Questões legais e éticas, especialmente no que diz respeito ao uso de biometria e ao monitoramento por câmeras, exigem a conformidade com leis de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil (Nogueira, 2021). A integração com sistemas legados também pode ser complexa e exigir consultoria especializada.

3.PROCEDIMENTOS METODOLÓGICOS

Este estudo baseia-se em uma pesquisa bibliográfica, que, de acordo com Gil (2008, p. 50), é "desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos". A escolha por essa metodologia se justifica pela natureza do tema, que visa consolidar e sintetizar o conhecimento existente sobre a aplicação de sistemas integrados de portaria em ambientes industriais, em vez de gerar dados primários. O propósito é oferecer um panorama abrangente e fundamentado, compilando as principais contribuições de autores renomados para construir uma base teórica sólida.

O processo de pesquisa bibliográfica foi dividido em etapas sistemáticas para garantir a abrangência e a relevância das fontes. Inicialmente, realizou-se um levantamento exploratório em bases de dados acadêmicas, como o Google Scholar, Scielo e periódicos da Capes, utilizando palavras-chave como "segurança industrial", "sistemas de controle de acesso", "automação de portaria" e "tecnologia em plantas industriais". Essa etapa inicial permitiu identificar os autores mais citados e os temas recorrentes na literatura, direcionando o foco da pesquisa para as obras de maior impacto.

A segunda etapa envolveu a seleção criteriosa das fontes. Foram priorizados livros clássicos e referências metodológicas (Gil, 2008; Lakatos; Marconi, 2010) que servem de alicerce para a pesquisa científica. Em seguida, foram selecionados artigos científicos recentes, publicados nos últimos cinco anos, para garantir que a discussão sobre tecnologias e tendências estivesse atualizada. Além disso, a pesquisa incluiu a consulta a normas técnicas e regulamentadoras, como a NR-33, que trata de segurança em espaços confinados, e a ISO 31000, sobre gestão de riscos, a fim de contextualizar a teoria com as exigências práticas e legais do setor.

Para cada fonte selecionada, foi realizada a leitura analítica e a extração de informações relevantes. As principais ideias e conceitos de cada autor foram sintetizados e organizados por subtópicos, permitindo a construção do referencial teórico de forma lógica e coesa. Essa abordagem, conforme Lakatos e Marconi (2010), é fundamental para que o pesquisador possa identificar pontos de convergência e divergência entre as perspectivas dos autores, enriquecendo a discussão e a análise dos resultados. Não houve coleta de dados de campo ou entrevistas, o que diferencia este estudo de uma pesquisa empírica ou de um estudo de caso.

A última etapa metodológica consistiu na elaboração da seção de resultados e discussão, na qual os achados da revisão bibliográfica foram sintetizados e interpretados. O objetivo foi demonstrar como a literatura consultada responde à questão central do estudo: como os sistemas integrados de portaria contribuem para a segurança e eficiência das plantas industriais. Essa etapa permitiu que a pesquisa fosse além da mera compilação de informações, oferecendo uma análise crítica e conclusiva sobre o tema, com base nas evidências encontradas nas obras e nos artigos consultados.

4.RESULTADOS

A análise da vasta literatura revisada demonstrou uma clara e inequívoca superioridade dos sistemas integrados de controle de portaria em relação aos métodos tradicionais de segurança. O principal achado da pesquisa é que a integração tecnológica não se limita a somar funcionalidades, mas sim a criar uma sinergia que eleva a eficácia da segurança a um patamar exponencialmente mais alto.

Essa transição de uma portaria reativa para uma proativa é o cerne da modernização da segurança industrial, uma visão corroborada por Machado (2020), que ressalta como a conectividade entre diferentes sistemas permite uma visão holística e em tempo real do ambiente fabril.

Um dos resultados mais evidentes da implementação desses sistemas é a notável redução de vulnerabilidades humanas. Enquanto a portaria tradicional está sujeita a falhas como o erro de digitação, a perda de um crachá ou a distração do operador, os sistemas automatizados minimizam esses riscos. A biometria, por exemplo, oferece um nível de segurança que a credencial física não pode garantir, pois a identificação biométrica não pode ser roubada, clonada ou falsificada (Pereira, 2018). Essa robustez na autenticação é vital para a proteção de áreas sensíveis, como laboratórios de P&D, salas de controle ou depósitos de materiais perigosos.

Além da autenticação, a capacidade de rastreabilidade e auditoria é um resultado fundamental. Cada acesso, seja de pessoa ou veículo, é digitalmente registrado no software de gestão, criando um banco de dados completo e imutável.

Essa trilha de auditoria é inestimável em caso de incidentes de segurança, permitindo aos gestores identificar rapidamente quem acessou uma determinada área em um horário específico. Essa funcionalidade não apenas facilita a investigação, mas também serve como uma poderosa ferramenta de compliance com normas de segurança internas e externas, como as exigências de órgãos reguladores (Silva, 2019).

A eficiência operacional emerge como um resultado diretamente mensurável da automação. A revisão da literatura aponta que a automação dos processos de entrada e saída elimina gargalos logísticos.

O uso de leitores de RFID para veículos pesados, por exemplo, permite que caminhões acessem o pátio de carregamento sem a necessidade de um registro manual demorado, reduzindo filas e o tempo de inatividade. Essa otimização de fluxo de pessoas e veículos tem um impacto direto na produtividade e na competitividade da empresa, conforme sublinhado

por Moraes (2015). A rapidez no acesso traduz-se em maior fluidez para a cadeia de suprimentos.

O papel dos sistemas de gestão de segurança (SMS) como um ponto central de comando é outro resultado crucial. A integração de câmeras de CFTV com sensores de alarme e controle de acesso permite que a equipe de segurança monitore e gerencie toda a planta a partir de uma única interface.

Em caso de uma tentativa de intrusão, o sistema pode acionar alarmes sonoros e visuais, fechar portões e direcionar as câmeras para o ponto de ocorrência de forma automática. Essa capacidade de resposta coordenada e imediata minimiza o tempo de reação e aumenta a eficácia da equipe de segurança, salvaguardando vidas e ativos.

A discussão sobre o tema também revela a importância do planejamento estratégico na implementação. A literatura aponta que os custos iniciais de investimento em hardware e software são uma barreira para muitas empresas, mas a análise de custo-benefício mostra que o retorno sobre o investimento (ROI) se manifesta em ganhos a longo prazo. Nogueira (2021) argumenta que o ROI pode ser calculado pela redução de perdas por furtos, a diminuição de acidentes de trabalho e a otimização de processos, que levam a um aumento de produtividade. Esses benefícios intangíveis, mas mensuráveis, justificam o investimento inicial.

Um dos resultados mais instigantes da pesquisa é a crescente tendência da análise preditiva na segurança industrial. O estudo de Souza (2022) destaca o uso de Inteligência Artificial (IA) para analisar padrões de comportamento de acesso e identificar anomalias. Por exemplo, se um funcionário acessa uma área restrita em um horário incomum, o sistema pode sinalizar o evento como suspeito, mesmo que o acesso seja tecnicamente permitido. Essa capacidade de antecipar riscos e atuar preventivamente é a próxima fronteira da segurança, transformando a portaria de um ponto de controle para um centro de inteligência estratégica.

A revisão também evidenciou que a implementação de sistemas de portaria integrada vai além da tecnologia, exigindo uma mudança cultural e um planejamento robusto. É crucial que a organização invista em treinamento de pessoal para que os colaboradores compreendam e operem o sistema corretamente. Além disso, a conformidade com leis de proteção de dados, como a LGPD, é um aspecto fundamental, especialmente no uso de dados biométricos. A falta de políticas claras de privacidade pode levar a problemas legais e éticos, comprometendo a confiança dos colaboradores e a reputação da empresa.

A análise da literatura demonstra que os sistemas integrados de portaria são uma solução robusta e moderna para os desafios de segurança e eficiência em plantas industriais.

ISSN- 2966-0785 REVISTA ACADÊMICA DA LUSOFONIA

Eles transformam a portaria de um ponto de controle estático em um centro de inteligência operacional, capaz de gerenciar riscos, otimizar processos e fornecer dados valiosos para a tomada de decisões estratégicas. A integração de tecnologias como biometria, RFID e CFTV, gerenciadas por um software central, cria um ecossistema de segurança que é superior, em todos os aspectos, aos métodos tradicionais.

Ademais, o objetivo principal do controle de acesso é a segurança de um local e de pessoas, no intuito a proteção contra invasões, roubos e vandalismo. Ao restringir o acesso a áreas sensíveis, o controle de acesso ajuda a prevenir incidentes de segurança.Nas atividades de uma indústria de fabricação de produtos, relatar o controle de portaria em relação à pesagem de entrada de caminhões com matérias-primas ou embalagens e saída de caminhões carregados com produtos fabricados, envolve alguns passos importantes.

Outra responsabilidade é gerar relatórios periódicos sobre as movimentações de entrada e saída, incluindo pesos, tipos de carga e outras informações relevantes. Isso ajuda na gestão da produção e no controle de estoque.Manter um registro detalhado de todos os caminhões que entram e saem da indústria, incluindo data, hora, tipo de carga (matérias-primas, produtos fabricados, embalagens), peso da carga e identificação do motorista e do veículo.

A verificação de documentos também é essencial para o bom andamento da planta, se todos os documentos necessários (como notas fiscais, ordens de compra, ordem de carga, etc.) estão em ordem para as entradas e saídas de caminhões.Para intensificar esse controle usar o POPs- procedimentos operacionais padrão. Para garantir que todos os funcionários sigam os mesmos procedimentos para controle de portaria e pesagem.

Além disso, o controlador de acesso orienta e encaminha as pessoas para os locais desejados garantindo a segurança e ordem no local, tomando medidas para prevenir a entrada de pessoas não autorizadas.

No controle de acesso físico podem ser usados dispositivos como catracas, leitores de cartão ou coletores de pontos, com leitura digital ou reconhecimento facial, bem como o sistema de integrado de câmeras de vigilância.

Já o controle lógico se aplica a sistemas de segurança de informações digitais, impedindo que pessoas não autorizadas acessem dados confidenciais ou redes de uma empresa. Não sendo de autorização necessariamente de acesso aos porteiros, mas sim de um superior como encarregado do setor.

ISSN- 2966-0785 REVISTA ACADÊMICA DA LUSOFONIA

Aos procedimentos de recebimento de visitas, o porteiro deve solicitar a identificação do visitante, seja por meio de um documento de identidade ou de uma credencial de visita. Deve-se registrar a entrada do visitante em um livro de registro ou em um sistema de gerenciamento de acesso.

Comunicar a chegada do visitante ao responsável pela área ou ao funcionário que o visitante deseja visitar, acompanhar o visitante até a área designada ou até o local de encontro com o funcionário.

Isso deve ser feito com base nas permissões pré-estabelecidas, horários e níveis de acesso permitidos de acordo com as regras de segurança da empresa, mediante agendamentos, excerto em inspeções federais e auditorias

Três processos formam a base de um controle de acesso seguro e eficiente, sendo eles autenticação, autorização e auditoria e devem estar alinhados com as políticas da empresa e normas de conformidade.

Dentre os dispositivos tecnológicos mais utilizados, destaca-se a biometria sendo eficácia por conter características físicas humanas únicas. Mas também são muitos utilizados outros dispositivos, como cartões de aproximações, reconhecimento facial, por ires, senhas smartphones com tecnologias via bluetooth, NFC-Near Field Communication e até mesmo por identificação por veias em leitores de impressões.

Implementação de controle de acesso, deve se utilizar de software eficiente e seguir algumas etapas de validação, avaliação de riscos, escolher dispositivos e tecnologia.As políticas de segurança da empresa, através da documentação dos padrões de segurança, governam o uso de controles de acesso.

Os controles de acesso podem ser divididos em dois tipos os quais são procedimentais ou propriamente ditos. Os controles de acesso procedimentais são restrições impostas por procedimento através de informações, treinamentos, ou mesmo controlado somente por alguma pessoa como segurança, porteiro ou recepcionista o reconhecimento e controle das pessoas é feito por crachás, credenciais, passes de trânsito livre, código de cores etc.

Os controles de acesso propriamente ditos são meios que estabelecem restrições à circulação e/ou acesso. Este tipo de controle é o que nos interessa, pois nele estão contidas, em conjunto com a ação humana, barreiras físicas que restringem acesso a determinadas áreas.

Apesar dos desafios de implementação, os resultados da pesquisa indicam que os benefícios a longo prazo, tanto em segurança quanto em produtividade, superam os custos e as complexidades. A transição para um modelo de segurança integrado é um passo inevitável

para as indústrias que buscam se manter competitivas e resilientes em um cenário de crescentes riscos e demandas por eficiência. A portaria, que antes era a entrada da fábrica, hoje se consolida como a porta de entrada para a era da segurança inteligente.

5 CONSIDERAÇÕES FINAIS

O presente estudo bibliográfico alcançou seu objetivo de analisar a contribuição dos sistemas integrados de controle de portaria para a segurança e a eficiência de plantas industriais. A pesquisa demonstrou que a integração de tecnologias como biometria, RFID e softwares de gestão oferece uma solução robusta para os desafios de segurança, mitigando riscos, otimizando o fluxo de pessoas e veículos e fornecendo dados estratégicos para a gestão. O estudo ressalta que, apesar dos desafios de custo e implementação, os benefícios a longo prazo, como a redução de perdas e o aumento da produtividade, justificam o investimento.

A principal contribuição deste trabalho é a consolidação de um referencial teórico que demonstra o valor da automação e da tecnologia na segurança industrial. O artigo reforça a transição de portarias meramente funcionais para centros de inteligência e controle, que atuam como o primeiro ponto de defesa de uma planta industrial. Essa mudança de paradigma é essencial para que as empresas modernas possam enfrentar os desafios complexos de segurança e se manterem competitivas. A portaria, nesse contexto, deixa de ser um mero posto de vigilância e se torna um elemento estratégico para a resiliência e a continuidade operacional do negócio.

A pesquisa também evidenciou que a implementação de sistemas integrados não é um processo puramente tecnológico, mas uma jornada que exige planejamento estratégico e uma cultura organizacional de segurança. A conformidade com a LGPD no uso de dados biométricos e de videomonitoramento, bem como o investimento em treinamento de pessoal, são fatores críticos de sucesso. A falha em abordar esses aspectos pode comprometer a eficácia do sistema e gerar problemas legais e éticos. Portanto, a tecnologia é apenas uma parte da solução, sendo o planejamento e a gestão os pilares que sustentam a sua real eficácia.

A principal limitação deste estudo é a ausência de dados empíricos de caso, o que impede a mensuração quantitativa do impacto desses sistemas em uma empresa específica. Embora a pesquisa bibliográfica forneça uma base teórica sólida, a aplicação prática e os resultados financeiros de uma implementação real permanecem como um campo a ser

explorado. O estudo, por ser de natureza secundária, se baseia na experiência de outros pesquisadores, sem a possibilidade de validação direta das hipóteses em um ambiente real.

Considerando as lacunas identificadas, sugere-se, como pesquisa futura, a realização de um estudo de caso em uma planta industrial que tenha implementado um sistema de portaria integrada. Tal pesquisa poderia utilizar metodologias mistas, combinando a análise de dados quantitativos (como tempo de acesso, incidentes de segurança antes e depois da implementação) com entrevistas qualitativas com gestores e colaboradores. Esse tipo de estudo permitiria validar as premissas teóricas aqui apresentadas e fornecer uma base de evidências concreta para futuras decisões de investimento em tecnologia de segurança.

REFERÊNCIAS

FISCHER, R. **Segurança industrial: guia para gestores**. 2. ed. Rio de Janeiro: Editora Cidadela, 2007.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de metodologia científica**. 7. ed. São Paulo: Atlas, 2010.

MACHADO, R. S. **Automação e segurança em ambientes industriais**. 3. ed. São Paulo: Editora Técnica, 2020.

MORAES, F. A. **Gestão de portaria em condomínios e indústrias**. Rio de Janeiro: Editora Expressão, 2015.

NOGUEIRA, L. M. **A Lei Geral de Proteção de Dados (LGPD) e o monitoramento no ambiente de trabalho**. São Paulo: Revista de Direito Digital, 2021.

PEREIRA, J. V. **Tecnologias de controle de acesso: um olhar sobre a biometria e RFID**. Revista de Engenharia Eletrônica, v. 15, n. 2, p. 45-60, 2018.

SILVA, D. R. **Vulnerabilidades e riscos em plantas industriais**. 1. ed. Curitiba: Editora Conhecimento, 2019.

SOUZA, M. L. **O futuro da segurança industrial: IoT, IA e análise preditiva**. Revista de Automação Industrial, v. 9, n. 4, p. 110-125, 2022.