Industrialização, Digitalização, Desempenho

5º Simpósio Brasileiro de Tecnologia da Informação e Comunicação na Construção e 5º Workshop de Tecnologia de Processos e Sistemas Construtivos

FLORIANÓPOLIS-SC | 20 a 22 de agosto

[1]FRAMEWORK PARA A MODELAGEM E SIMULAÇÃO DE ATAQUES CIBERFÍSICOS EM EDIFICAÇÕES COM USO DA BIM

Framework for modeling and simulating cyber-physical attacks in buildings utilizing the BIM

Christiana Couto
Instituto Militar de Engenharia | Rio de Janeiro, RJ | christianacouto@ime.eb.br

Giuseppe Miceli Junior
Instituto Militar de Engenharia | Rio de Janeiro, RJ | giuseppe.pged.@ime.eb.br

Gabriela Moutinho de Souza Dias
Instituto Militar de Engenharia | Rio de Janeiro, RJ | gabriela@ime.eb.br

Ronaldo Moreira Salles
Instituto Militar de Engenharia | Rio de Janeiro, RJ | salles@ime.eb.br

RESUMO

Os ataques ciberfísicos começam no mundo cibernético, mas trazem consequências para o mundo físico. Por isso, os profissionais e pesquisadores vêm desenvolvendo novas técnicas para proteger as edificações. A modelagem e simulação desses ataques permite aos profissionais da construção visualizar e estimar as suas consequências para elaborar defesas para as edificações. Essa abordagem, é melhor se feita desde a fase de planejamento comparado a implementação em fases posteriores. Contudo, não existe ainda um software no mercado que ofereça a modelagem e a simulação de ataques ciberfísicos de forma integrada. Portanto, para preencher essa lacuna, este trabalho apresenta um framework para modelar e simular ataques ciberfísicos, utilizando a Building Information Modeling (BIM), dividido nas fases: pessoas, processos e tecnologias. Primeiramente, o modelo da edificação é utilizado como entrada para as simulações, que permitem a análise sob diferentes cenários, para vários ataques, e os resultados servem de referência para a elaboração de técnicas de defesa. O framework apresentado neste trabalho inova ao implementar a segurança contra ataques ciberfísicos aproveitando a familiaridade dos profissionais, as ferramentas e outros recursos da metodologia BIM. Foi realizado um estudo de caso para a proteção de um depósito de armamentos e munição.

Palavras-chave: ataques ciberfísicos, segurança da informação, building information modeling (BIM), modelagem, simulação

ABSTRACT

Cyber-physical attacks begin in the cyber world but have consequences for the physical world. Therefore, professionals and researchers have been developing new techniques to protect buildings. Modeling and simulating these attacks allows construction professionals to visualize and estimate their consequences in order to develop defenses for buildings. This approach is best done from the planning phase rather than implementing them in later phases. However, there is still no software on the market that offers modeling and simulation of cyber-physical attacks in an integrated way. Therefore, to fill this gap, this paper presents a framework for modeling and simulating cyber-physical attacks, using Building Information Modeling (BIM), divided into the following phases: people, processes and technologies. First, the building model is used as input for the simulations, which allow analysis under different scenarios, for various attacks, and the results serve as a reference for the development of defense techniques. The framework presented in this paper innovates by implementing security against cyber-physical attacks taking advantage of the professionals' familiarity with the tools and other resources of the BIM methodology. A case study was carried out for the protection of an arms and ammunition depot.

Keywords: *Ciber-physical attacks, Information Security, Building Information Modeling (BIM), Modeling; Simulation*

1 INTRODUÇÃO

Sistemas ciberfísicos conectam equipamentos físicos, como atuadores e sensores, a sistemas cibernéticos (Refsdal, 2015). Sistemas ciberfísicos são diferentes dos tradicionalmente estudados na tecnologia da informação por criarem uma conexão entre o mundo virtual e físico. Assim, ataques ciberfísicos exploram vulnerabilidades tanto no mundo virtual quanto no mundo físico. O seu objetivo é causar danos físicos ou disrupção das operações dos sistemas. Dado o crescente aumento dos ataques ciberfísicos em edificações, pesquisadores vêm estudando mais sobre como criar técnicas de defesa para protegê-los.

[1]COUTO, C.; MICELI JUNIOR, G. DIAS, G. M. S.; SALLES, R. M. Framework para a Modelagem e Simulação de Ataques Ciberfísicos em Edificações com uso da BIM. In: 5º SIMPÓSIO BRASILEIRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO NA CONSTRUÇÃO, 4., 2025, Florianópolis. **Anais [...].** Porto Alegre: ANTAC, 2025.

Nos estudos de técnicas de defesas para proteger as edificações, também pode-se optar por realizar testes in loco ou utilizar simulações. Ao optar por simulações ao invés de experimentos físicos, são evitados custos e danos às próprias edificações. Contudo, há desafios para a modelagem, simulação e experimentação dadas as suas particularidades (NEVES, 2014).

Os desafios são a integração das características físicas e cibernéticas e, em um contexto de ataques a diferentes tipos de infraestruturas, modelar essa heterogeneidade. Por isso, este trabalho faz um recorte para o estudo somente de edificações, dado que a modelagem nessa área está mais unificada, e se difere muito de outras áreas, como rodovias e ferrovias.

A principal diferença entre a modelagem de ataques ciberfísicos e cibernéticos está nos elementos físicos. Enquanto na modelagem dos ataques cibernéticos não se consideram propriedades físicas como material, tamanho e distância, na modelagem dos ataques ciberfísicos, essas características são de suma importância. Como exemplo, Oliveira (2024) realizou um estudo sobre diversos ataques em subestações digitais, mas não incluiu as características físicas das subestações, nem das linhas de transmissão. Por isso, foi sugerido, como trabalho futuro, a consideração dos aspectos físicos dos sistemas elétricos, frente a diferentes cenários, para avaliar os ataques de forma mais sistêmica. É importante considerar essas informações nas simulações dos ataques ciberfísicos, especialmente nesse caso, dada a defasagem temporal causada pela distância, da ordem de quilômetros, entre as linhas de transmissão.

As principais métricas de interesse nesses estudos são os custos financeiros resultantes dos ataques e seu tempo de duração. Existem muitas ferramentas no mercado para estudo de ataques cibernéticos, que não possuem impacto no mundo físico, que utilizam essas medidas, como o SecuriCAD, criado por Ekstedt et al. (2015). Apesar de incluírem diversos ataques e dispositivos de tecnologia da informação e comunicação, não incluem as características físicas das edificações.

Para solucionar esse problema, ferramentas como o ASTORIA, criada por Wermann et al. (2016) foram desenvolvidas para ataques ciberfísicos, mas somente para infraestruturas específicas. Os autores criaram um framework para simulação de ataques ciberfísicos em smart grids utilizando softwares já disponíveis no mercado. Além disso, realizaram estudos de diferentes cenários para vários ataques. Contudo, não é possível utilizar esse framework para outras infraestruturas porque se baseia em componentes específicos do setor elétrico. Da mesma forma, Oliveira (2024) também se limitou ao setor elétrico.

Em suma, ainda não há um framework padrão para o estudo dos ataques ciberfísicos, em diferentes contextos de infraestruturas, no Estado-da-Arte. Mas existem vários estudos de ataques cibernéticos e alguns de ataques ciberfísicos em infraestruturas específicas. As vantagens do uso de modelagem e simulação para o estudo de ataques ciberfísicos em edificações são os seguintes:

- Emprego com baixo custo;
- Realização de testes em ambientes de construção que ainda estão em fase de planejamento;
- Proteção ao ambiente por não causar danos;
- Escalabilidade do número de experimentos;
- Possibilidade de simular uma variedade de condições e cenário que poderiam ser difíceis ou inviáveis de replicar em experimentos físicos;
- Segurança nos testes ao evitar consequências físicas;
- Flexibilidade de ataques e cenários;
- Facilitação da reprodutibilidade dos experimentos dando mais rigor científico;
- Aumento da fidelidade dos modelos ao incluir as características físicas.

Por outro lado, os desafios tecnológicos são que não há uma ferramenta padrão para realizar a modelagem e a simulação dos ataques ciberfísicos nem um processo definido para realizar o estudo. Existem diversas abordagens diferentes no Estado-da-Arte mas nenhuma está consagrada.

Por outro lado, já existem diversas ferramentas para modelar edificações. O setor de Arquitetura, Engenharia, Construção e Operação (AECO), já se aproveita da gama de recursos disponíveis pela Modelagem da Informação da Construção (BIM) (Succar, 2008). A adoção da BIM é motivada pela variedade de aplicações que permitem alcançar diversos objetivos no setor da construção, tais como modelagem 3D, detecção de interferências, trabalho colaborativo, simulações energéticas, análise de custos, planejamento e visualização para construção ou fabricação (Ahn et al., 2013).

Por exemplo, para o caso de subestações elétricas, como a realizada por Oliveira (2024), pode-se analisar os efeitos dos ataques também nas casas alimentadas pelas subestações e o tempo de propagação da falha elétrica. Assim, poderia-se calcular quantas residências ficariam sem energia e por quanto tempo.

Como resultados das simulações, as métricas de interesse são os custos resultantes dos ataques e seu tempo de duração, de forma similar a outros trabalhos de simulações com BIM (Cursino et al., 2021).

Do ponto de vista de pessoas, os desafios para elaboração do framework proposto são o desconhecimento dos profissionais do setor de AECO com o tema e a participação dos especialistas em segurança física que aumentam os custos.

Foram estudados trabalhos relacionados a fim de se compreender como a BIM é utilizada, integrada a inovações tecnológicas, para outras finalidades. A integração de softwares BIM, com outras ferramentas, a fim de expandir as suas funcionalidades, cresceu muito desde o advento do padrão Industry Foundation Classes (IFC) (Moura et al., 2024). Foram identificadas tecnologias como: inteligência artificial (Alves et al., 2023), gêmeos digitais (Galvão et al., 2023), Blockchain (Piccoli et al., 2023), realidade virtual e aumentada (Silva et al., 2021), simulação energética (Cortês et al., 2021) e sistemas de informações geográficas (GIS) (Cursino et al., 2021).

Além disso, aplicações da BIM em outras áreas interligadas à segurança da informação como segurança do trabalho (Martins et al., 2021), prevenção a desastres naturais (Cursino et al., 2021) e gestão de ativos (Otranto et. al, 2025) também foram estudadas. Por exemplo, a BIM já foi amplamente utilizada para o desenvolvimento de técnicas de defesa para proteger a vida humana em situações de desastres naturais. Cursino et al. (2021) propuseram o uso de softwares BIM integrados a GIS para mitigar riscos de enchentes em áreas urbanas. Ao realizar várias simulações, é possível realizar diversas análises e elaborar alternativas de construção segura para o projeto do planejamento urbano. Como resultado, foram definidos indicadores de custo e prazo e elaborados estudos preliminares.

Sobre a segurança do uso da BIM em si, Dos Santos et al. (2021) levantaram uma reflexão sobre a importância da gestão e segurança da informação. Mas o foco do seu trabalho foi uma abordagem para segurança das informações, dos projetos dos empreendimentos, no modo como são obtidas, criadas, processadas, compartilhadas e/ou armazenadas, ao longo do ciclo de vida das edificações. Este trabalho, por outro lado, estuda a segurança das próprias edificações contra ataques ciberfísicos.

Além disso, o BIM está intrinsecamente relacionado com frameworks (Nielsen et al., 2023b). Baseando-se nesses resultados, entende-se que incluir o BIM na elaboração de um framework para modelagem e simulação de ataques ciberfísicos em edificações é promissor.

Portanto, este trabalho investiga o uso da BIM para corrigir a lacuna existente de modelagem das características físicas das edificações nas simulações de ataques ciberfísicos. Ao utilizar os modelos BIM como ponto de partida para as simulações de ataque, pode-se detalhar mais as características físicas das edificações, nos mesmos moldes da modelagem da indústria AECO. Assim, pode-se visualizar e calcular os efeitos dos ataques em mais detalhes. Além disso, pode-se utilizar modelos de qualquer infraestrutura, para qualquer setor, sem as limitações enfrentadas pelos outros trabalhos relacionados.

Neste contexto, o presente artigo propõe um framework para modelagem e simulação de ataques ciberfísicos em edificações utilizando o BIM, composto pelas seguintes etapas: pessoas, processos e tecnologias.

2 METODOLOGIA

Para desenvolvimento do framework proposto foi utilizada a metodologia *design science research* (DSR) dado que o artefato, o framework proposto, do tipo método de integração, possui uma natureza aplicada. Foi seguido o fluxo proposto por Dresch et al. (2015) para operacionalizar o DSR.

A implementação se deu, primeiramente, pela identificação do problema, conscientização do problema e revisão bibliográfica que estão apresentadas na seção de introdução. Em seguida, a etapa de projeto e desenvolvimento do artefato é apresentada na seção 3, na qual, as etapas do framework proposto estão descritas. Posteriormente, o artefato é validado por meio de um estudo de caso, os resultados são apresentados e discutidos na seção 4. Finalmente, as conclusões finais são abordadas na última seção.

3 RESULTADOS E DISCUSSÃO

Primeiramente, diversas perguntas devem ser investigadas para a modelagem e simulação de ataques ciberfísicos, dentre as quais:

1. Quais são os principais alvos dos atacantes?
2. O que se quer proteger?
3. Quais os locais de maior interesse para os atacantes?
4. Quais as técnicas de ataque que os atacantes podem utilizar? Quais os equipamentos?
5. Quais são os mecanismos de defesa que já estão presentes ou podem ser adquiridos para a proteção da edificação?
6. Quais as técnicas de defesa que podem ser utilizadas?

Deve-se pensar, primeiramente, nas características dos ataques, para depois projetar as defesas em conformidade. Por exemplo, em um mesmo ambiente, identifica-se quais as possibilidades de entrada e fuga, quais os objetos de maior interesse para destruição ou roubo, quais as ferramentas que os atacantes podem utilizar, etc.

As técnicas de defesa a serem incorporadas na edificação podem incluir orientação da construção, barreiras, esconderijos, rotas de fuga, além de equipamentos como câmeras de monitoramento, sensores de movimento, sinais de aviso, detectores de fumaça, portas automáticas e blindadas, disjuntores, alarmes e outros.

Nessa linha, já existem várias opções no BIM para famílias de elementos de segurança e de alvos de ataques como cofres e armários de armamentos e munições.

Além disso, ao utilizar o BIM no estudo de ataques ciberfísicos em edificações, pode-se aproveitar muitas outras vantagens, como a familiaridade dos profissionais da indústria AECO. A fim de expandir as suas funcionalidades, essa alternativa para aumentar a segurança da edificação se torna mais uma opção para os projetistas durante a fase de projeto (Miceli Junior, 2019a, Ahn et al., 2013).

Além de recursos, também já existem normativas sobre o tema. Nesse contexto, a ISO 19650-5 “Organização e digitização da informação sobre edifícios e obras de engenharia civil, incluindo modelagem da informação da construção (BIM) - parte 5”, fornece uma estrutura para as organizações entenderem as questões de vulnerabilidade e os controles de segurança para ambientes construídos, ativos, produtos, serviços, indivíduos ou comunidades, e informações associadas, numa abordagem voltada à segurança.

Segundo a ISO 19650-5, ao iniciar o desenvolvimento de uma abordagem voltada à segurança, uma iniciativa, empreendimento, ativo, produto ou serviço planejado, deve começar já nas etapas de planejamento. Por isso, este trabalho é voltado para permitir modificações já na fase projeto através de simulações de ataques ciberfísicos.

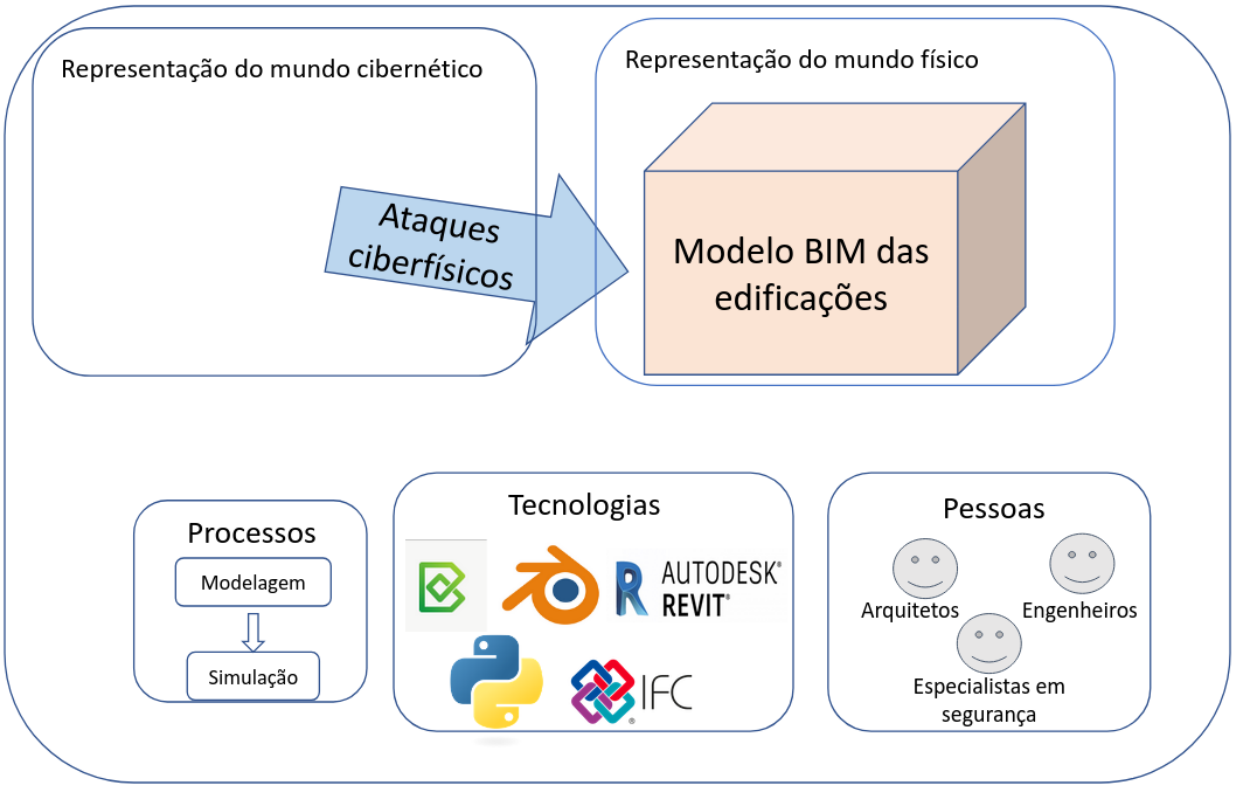
Além disso, o BIM está intrinsecamente relacionado com frameworks, como mostra o trabalho de Nielsen et al. (2023b). Esse termo foi um dos mais frequentes encontrados na análise bibliométrica realizada pelos autores. Baseando-se nesses resultados, entende-se que incluir o BIM na elaboração de um framework para modelagem e simulação de ataques ciberfísicos em edificações é promissor.

Para utilizar o BIM neste trabalho, seguiu-se a linha definida por Messner et al. (2019). Primeiramente, a definição dos objetivos gerais da implantação do BIM é um dos passos mais importantes do processo de planejamento desses objetivos, que assim que definidos, delimitam os usos específicos do BIM. Uma vez que os objetivos forem definidos, as equipes de projeto devem identificar os usos BIM necessários para atingir os objetivos propostos.

Após identificar o uso do BIM para a finalidade deste trabalho, é essencial estabelecer os fluxos de trabalho, as trocas de informações necessárias e as responsabilidades de cada membro da equipe. Com essas informações bem delimitadas, é possível especificar as infraestruturas e tecnologias que darão suporte aos processos BIM a serem desenvolvidos.

Neste contexto, o presente artigo propõe um framework para modelagem e simulação de ataques ciberfísicos em edificações utilizando o BIM, composto pelas seguintes etapas: processos, tecnologias e pessoas, como mostra a Figura 1.

Figura 1: Framework proposto.



Fonte: Os autores

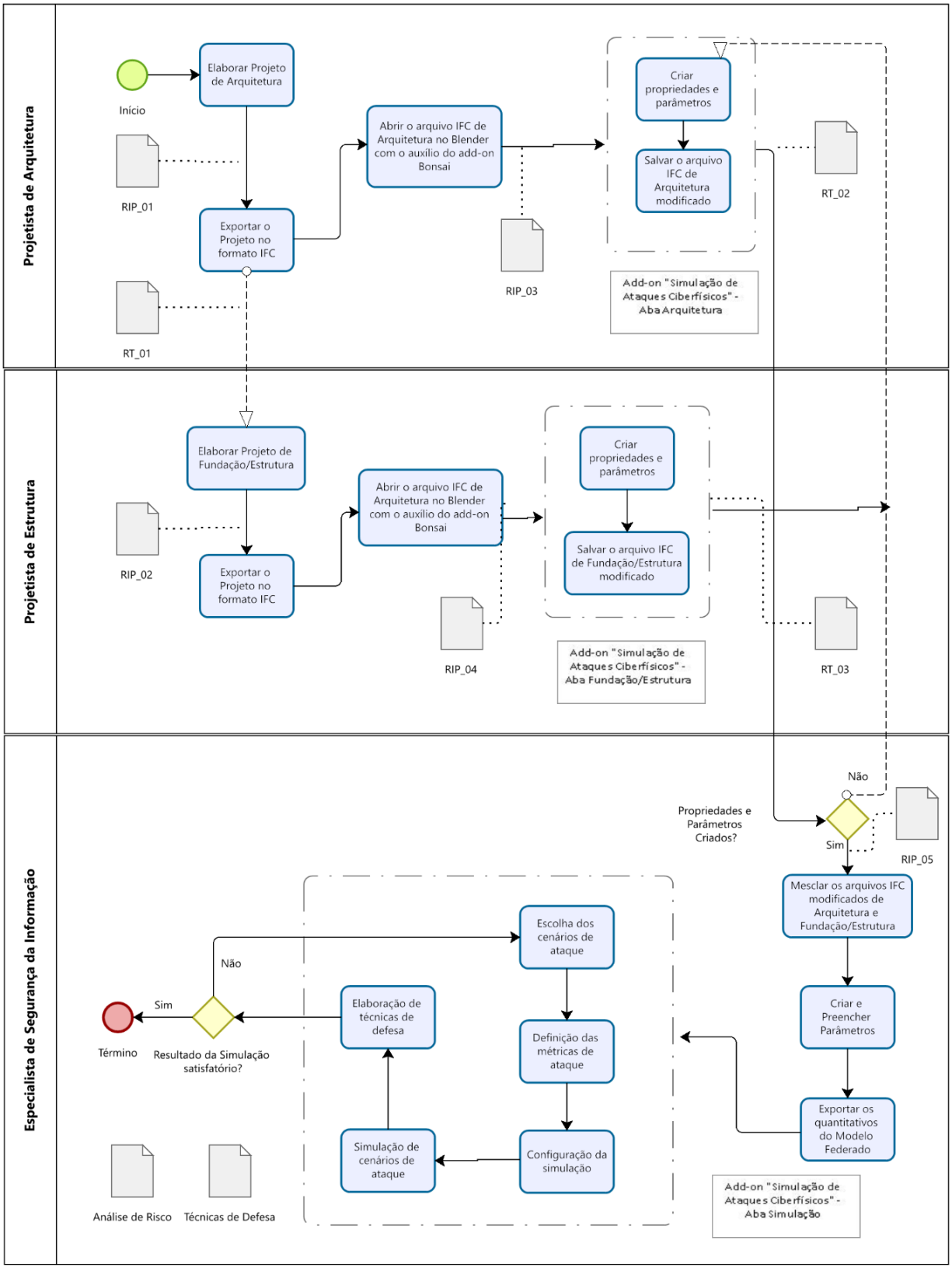
3.1 Processos

Foram selecionados trabalhos relacionados, no Estado-da-Arte, para compreender como são os processos "AS-IS" que utilizam BIM para estudos de ataques ciberfísicos nas edificações. Contudo, não há um processo "AS-IS" consagrado para este tipo de estudo. Só existem processos específicos para alguns tipos de edificações, como para proteção física de templos de cavernas (Chen et al., 2024), para proteção física de edifícios (Porter et al., 2014) e para sistemas de segurança contra acidentes em plantas petroquímicas (Dong et al., 2021). Por isso, foi feita a elaboração de um processo bem definido para preencher essa lacuna no Estado-da-Arte.

O fluxo de trabalho "*TO-BE*", proposto neste trabalho, integra a modelagem do projeto da edificação e a simulação de ataques ciberfísicos. A parte inicial do fluxo seguiu o trabalho de Moura et al. (2024), ao utilizar o modelo BIM como entrada para a modelagem. Contudo, já que os fluxos de trabalho devem ser específicos para cada objetivo a ser atingido, conforme Miceli Junior (2019b), a etapa de simulação para ataques ciberfísicos não tem qualquer correlação com a feita para orçamentação, de Moura et al. (2024). Este framework propõe um fluxo de trabalho específico para se estudar a segurança ciberfísica das edificações contra ataques ciberfísicos.

Para a elaboração do fluxo de trabalho, foi seguida a ISO 19650-3:2020 (ISO, 2020a), para a elaboração dos requisitos de informações organizacionais (OIR), de informações sobre ativos (AIR), de informações do projeto (RIP) e troca de informações (EIR) e dos modelos de informação do ativo (AIM) e modelo de informação do projeto (PIM). O fluxo de trabalho é descrito na Figura 2.

Figura 2: Fluxo de trabalho



Fonte: Adaptado de Moura et al. (2024).

Na Figura 2, são destacados os documentos trocados entre as partes interessadas, os RIP e requisitos de troca (RT), os entregáveis (a análise de risco e técnicas de defesa) e as atividades a serem desempenhadas

pelos projetistas BIM, de arquitetura e estrutura, e especialistas em segurança da informação. Para que a exportação do projeto BIM, no formato IFC, seja eficiente para a simulação de ataques ciberfísicos, o requisito de informação de projeto RIP_01 deve incluir informações obrigatórias e opcionais e unidades respectivas. As informações obrigatórias devem ser: nome, dimensões dos elementos, material, criticidade e valor. As opcionais devem ser descrição e tempo. A informação sobre o tempo só é necessária para equipamentos eletrônicos que possuem um tempo de atuação, como detectores de movimento, disjuntores e alarmes. As unidades de medida devem ter ordem de grandeza relacionada a edificação (comprimento em cm, área em m^2 e volume em m^3).

Da mesma forma, para o RIP_02, as informações obrigatórias devem ser nome, dimensões dos elementos, criticidade e valor. Como informação opcional, somente a descrição. Para o RIP_03, que contém as informações do projeto de arquitetura no formato IFC, segue-se a mesma linha. Posteriormente, no RIP_04 serão definidos os requisitos com informações do projeto estrutural, no formato IFC, que possibilita a simulação de ataques ciberfísicos. O RIP_05 contém as informações do modelo federado no formato IFC.

Depois de se elaborar os requisitos de informação, deve-se configurar os arquivos para exportação do software BIM.

Os requisitos de troca foram criados para garantir que os diferentes profissionais alinhem os seus trabalhos de acordo entre si. Para os módulos iniciais, foram criados os requisitos de troca RT_01, entre os projetistas de arquitetura e estrutural, para garantir que os projetos das disciplinas tenham o mesmo ponto de origem e sistema de unidades.

O RT_02 entre os projetistas de arquitetura e os especialistas em segurança da informação deve definir as propriedades e os parâmetros personalizados para os cenários de ataques ciberfísicos e o RT_03, da mesma forma, entre os projetistas de fundação/estrutura e os especialistas em segurança da informação.

Foram definidos dois entregáveis. Primeiro, um documento com as propostas de técnicas de defesa para aumentar a segurança da edificação contra ataques ciberfísicos seguindo um manual padrão. Isso foi pensado levando em consideração que o desenvolvimento de manuais de trabalho e processos bem estruturados para a integração dos profissionais da indústria AECO e dos de segurança da informação é um campo aberto. O segundo entregável do fluxo de trabalho é uma análise de risco sobre a situação da edificação “AS-IS”, seguindo um padrão também bem definido.

Além de recursos, também já existem normativas sobre o tema. Nesse contexto, a ISO 19650-5 “Organização e digitização da informação sobre edifícios e obras de engenharia civil, incluindo modelagem da informação da construção (BIM) - parte 5”, fornece uma estrutura para as organizações entenderem as questões de vulnerabilidade e os controles de segurança para ambientes construídos, ativos, produtos, serviços, indivíduos ou comunidades, e informações associadas, numa abordagem voltada à segurança (ISO, 2020b).

Segundo a ISO 19650-5, ao iniciar o desenvolvimento de uma abordagem voltada à segurança, uma iniciativa, empreendimento, ativo, produto ou serviço planejado, deve começar já nas etapas de planejamento. Por isso, este trabalho é voltado para permitir modificações já na fase projeto através de simulações de ataques ciberfísicos.

Como esses requisitos são específicos de cada projeto, será apresentado um estudo de caso como exemplo da implementação do framework proposto.

3.2 Tecnologias

Para criar uma solução completa de modelagem e simulação de ataques ciberfísicos em edificações, é necessário integrar diversas ferramentas. Os critérios utilizados para seleção das ferramentas foram interoperabilidade, código aberto e uso em larga escala. Nessa linha, conceito de OpenBIM que é uma iniciativa baseada em padrões abertos, como o IFC, para permitir interoperabilidade e modelagem colaborativa de fluxos de trabalho de forma agnóstica de softwares BIM, foi seguido para oferecer maior flexibilidade dentro das opções disponíveis no mercado.

O software Blender é gratuito, de código aberto e amplamente utilizado para animações, simulações, modelagem, renderização e etc. Inclui suporte com a linguagem de programação Python para o

desenvolvimento de programas independentes. O Blender possui compatibilidade com o BIM, a partir do padrão IFC. O Bonsai (anteriormente denominado BlenderBIM) é uma plataforma para o Blender que utiliza modelos BIM.

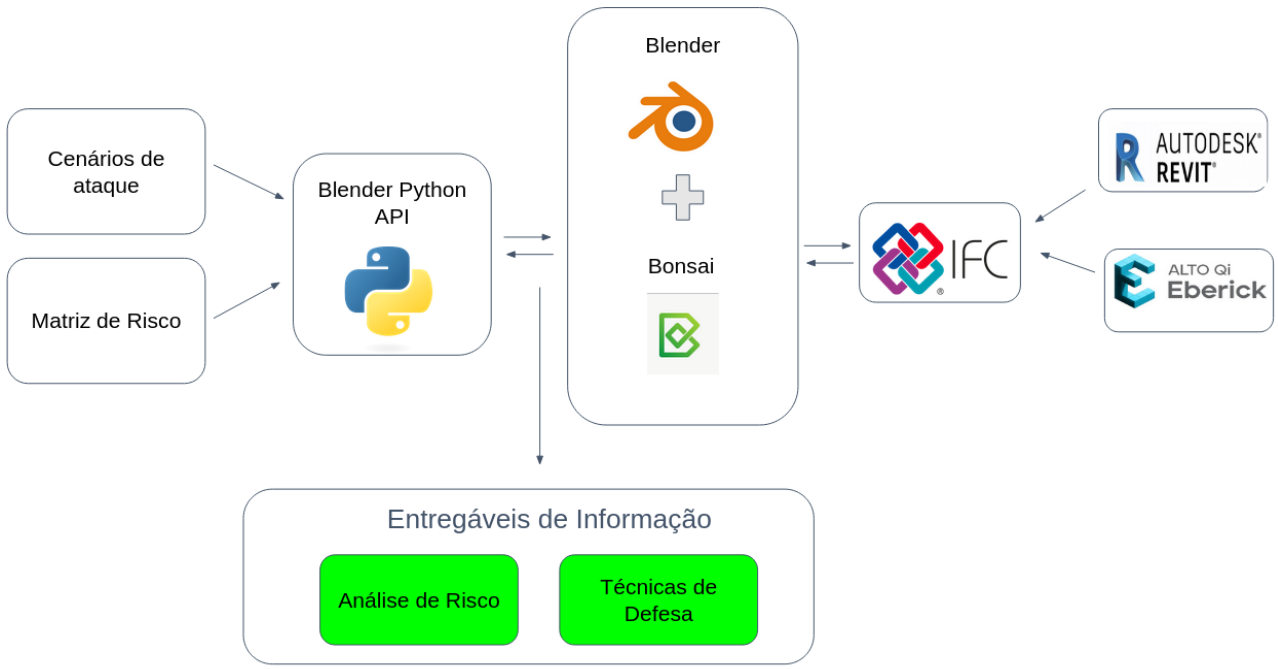
O uso do software Blender integrado ao BIM já foi explorado para aplicações em simulações energéticas por Godoi et al. (2023), para criar um fluxo de trabalho que integra a modelagem do projeto, fluxo de trabalho e elaboração de orçamentos, por meio do Sistema Nacional de Classificação, por Moura et al. (2024) e para gestão de ativos por Otranto et al. (2025).

Outros softwares voltados para segurança, utilizando BIM, também foram encontrados no Estado-da-Arte. Visando a segurança das pessoas que ocupam canteiros de obras, foi desenvolvido o Certus-HSBIM. Mas, apesar de os avanços no campo da segurança do trabalho estarem adiantados, ainda não há softwares voltados para segurança das edificações.

No Framework proposto, seguindo a linha de Moura et al. (2024), inicialmente cria-se o modelo BIM em uma ferramenta, como o Autodesk Revit, pelos projetistas e arquitetos. O modelo federado resultante é exportado para o Bonsai para permitir customizações específicas com a finalidade. Neste caso, simulações de ataques ciberfísicos. A linguagem Python é utilizada para criar os mecanismos por trás das simulações. Os especialistas de segurança da informação realizam diversas simulações, em diferentes cenários para vários ataques, para elaborar técnicas de defesa. Como resultado, os entregáveis são a análise de risco e propostas de técnicas de defesa.

A Figura 3 mostra o fluxograma para desenvolvimento deste artefato destacando as principais tecnologias adotadas.

Figura 3: Fluxograma para desenvolvimento do artefato



Fonte: Adaptado de Dresch et al. (2015).

A Tabela 1 descreve as tecnologias utilizadas no Framework, suas versões atuais, limitações e papel.

Tabela 1:Tecnologias utilizadas

Tecnologia	Versão atual	Papel	Limitação
Ferramentas BIM	Revit 2025	Modelagem das edificações	Não incluem simulações de ataques ciberfísicos.
Blender	4.4	Animação e simulação de ataques	Complexo para criar os modelos
IFC	4.3	Compatibilizar os modelos BIM com o Bonsai	Perda de dados.
Bonsai	0.8.0	Plataforma para integrar os modelos BIM ao Blender	
Python	3.14	Mecanismo por trás das simulações de ataques	Requer conhecimentos em programação e dificuldade para a criação de modelos em comparação com as ferramentas BIM.

Fonte: Os autores

3.3 Pessoas

É importante que os profissionais do setor de AECO se preparem para adotar medidas de proteção nos projetos e operações das edificações. Devem passar por uma capacitação para compreenderem a importância da segurança contra ataques ciberfísicos nas edificações.

Ao se incluir especialistas em segurança no setor de AECO, para trabalhar na elaboração de estudos sobre segurança ciberfísica das edificações, depara-se com problemas tradicionais do setor de tecnologia da informação em meio aos aumento de ataques: escassez de profissionais e alto custo da mão de obra especializada.

Dentro do modelo da equipe de implementação BIM apresentado por Nielsen et al. (2023a), já estão incluídos profissionais de tecnologia da informação. Mais especificamente, dada a especialização dos profissionais de segurança da informação, entende-se que deve-se definir seus papéis de forma separada.

3.4 Estudo de caso: depósito de armamentos e munição

Foi escolhido para o estudo de caso, um depósito de armamentos e munição. Segundo a ISO 19650-5, esse é um ativo construído considerado sensível porque cumpre função de segurança nacional.

Roubos são frequentes nos depósitos de armas e munições no Brasil: em 2023, no depósito de Barueri (EBC, 2023), em 2024, na Pavuna no Rio de Janeiro (O Globo, 2024) e, em 2024, as Forças Armadas da Ucrânia destruíram o maior depósito de munições da Rússia (Reuters, 2024).

Esses casos reais serviram de base para a definição dos cenários de ataque deste trabalho. Seguindo as etapas definidas no framework proposto para a equipe de segurança da informação foi criada a Figura 4. Os requisitos de informação de projeto, troca e de informação de ativos, estão mostrados nas Tabelas 2-6, conforme descrito na subseção 3.1.

Figura 4: Cenários do estudo de caso

	Cenário 1	Cenário 2
Objetivo	Invadir o depósito para roubo.	Explosão do depósito para destruição com fins militares;
Condições	1. Desativar ou contornar o sistema de monitoramento. 2. Ocultar o roubo das câmeras. 3. Abrir a sala cofre.	Os sistemas de monitoramento do espaço aéreo devem ser subjugados.
Equipamentos ciberfísicos envolvidos	1. Detectores de movimento 2. Alarmes 3. Câmeras de segurança 4. Trancas automáticas	Radares para monitoramento do tráfego aéreo e anti-mísseis.
Definição das métricas de ataque	1. Tempo de invasão 2. Quantidade de material roubado 3. Valor do material roubado 4. Número de portas abertas 5. Quantidade de salas invadidas 6. Distância entre a entrada e o objetivo final	1. Quantidade de aviões inimigos 2. Quantidade de paios destruídos 3. Quantidade de material bélico destruído 4. Valor do material destruído 5. Distância entre os aviões e o depósito
Elaboração das técnicas de defesa	1. Monitoramento por identificação automática dos equipamentos do depósito a fim de identificar e rastrear a carga roubada. 2. Utilizados dispositivos de rastreio e identificação como sistemas de identificação por radiofrequência. 3. Trancar automaticamente portas ao detectar movimento. 4. Acionar alarmes ao detectar movimento suspeito.	1. Monitoramento do tráfego aéreo e articulação com a força área para defesa. 2. Utilizar radares como primeira camada de defesa. 3. Acionar alarmes ao detectar movimento suspeito no espaço aéreo.

Fonte: Os autores

Tabela 2: Requisito de troca 2

Nome do requisito de troca	RT_02
Fase:	Fase de arquitetura
Disciplinas:	De: Arquitetura para: Avaliação de segurança
Descrição geral:	Requisito de troca aplica-se a fornecer ao analista de segurança, o projeto básico de arquitetura no formato IFC contendo propriedades e parâmetros personalizados que auxiliarão no estudo de segurança.
Descrição das informações:	1) As informações estão descritas nos Requisitos de Informação do Projeto RIP_03; 2) Sistema de unidade: comprimento (cm), área (m^2) e volume (m^3).

Fonte: Os autores

Tabela 3: Exemplo de RIP_03 para munições e armamentos

Nome do requisito de informação do projeto		RIP_03
Fase:	Fase de desenvolvimento do projeto	
Disciplinas:	Arquitetura	
Descrição geral:	Requisito de informação do Projeto que contém informações do Projeto de Arquitetura no formato IFC que possibilitem a análise de segurança.	
Tipo de ativos	Munições	Armamentos
Localização	Deodoro, RJ	Deodoro, RJ
Área	Paiol de munições	Paiol de armamentos
Material perigoso	Sim	Sim
Processo de end-of-life	Destruição	Destruição
Planos de emergência	Evacuação do ambiente e comunicação com o corpo de bombeiros	Evacuação do ambiente e comunicação com o corpo de bombeiros
Observações		

Fonte: Os autores

Tabela 4: Requisito de troca 3

Nome do requisito de troca	RT_03
Fase:	Fase de análise de segurança
Disciplinas:	De: Engenharia de custos para Avaliação de segurança
Descrição geral:	Requisito de troca aplica-se a fornecer ao analista de segurança, o projeto básico de fundação/estrutura no formato IFC contendo propriedades e parâmetros personalizados que auxiliarão no estudo de segurança.
Descrição das informações:	3) As informações estão descritas nos Requisitos de Informação do Projeto RIP_04; 4) Sistema de unidade: comprimento (cm), área (m²) e volume (m³).

Fonte: Os autores

Tabela 5: Exemplo de RIP_04 para munições e armamentos

Nome do requisito de informação do projeto	RIP_03
Fase:	Fase de desenvolvimento do projeto
Disciplinas:	Engenharia de estruturas
Descrição geral:	Requisito de informação do Projeto que contém informações do Projeto Estrutural no formato IFC que possibilitem a análise de segurança.
Unidades	Comprimento (cm), área (m²) e volume (m³).
Observações	

Fonte: Os autores

Tabela 6: Requisitos de Informações do Ativo (AIR)

Tipo de ativos
Localização
Área
Material perigoso
Processo de end-of-life
Planos de emergência
Fabricante
Número de identificação
Classificação
Marca e modelo
Informações de peças de reposição
Histórico de manutenção
Documentação de entrega/recebimento
Vida útil esperada
Custo

Fonte: Os autores

4 CONSIDERAÇÕES FINAIS

Este trabalho utiliza a BIM para corrigir a lacuna existente de modelagem das características físicas das edificações nas simulações de ataques ciberfísicos conforme o planejado. Ao utilizar os modelos BIM como ponto de partida para as simulações de ataque, detalhou-se mais às características físicas das edificações, nos mesmos moldes da modelagem já consagrada na indústria AECO.

As tecnologias utilizadas são abertas, tornando o custo reduzido. Por ser uma combinação de tecnologias já utilizadas no mercado, é necessário cuidado ao importar e exportar os dados e alguns requisitos de troca devem ser atendidos. Além disso, é necessário o desenvolvimento de um add-on específico para esse framework no Bonsai que deve ser mantido atualizado.

O exemplo de ataques em um depósito de armamentos e munições, mostrou o processo de implementação do framework, desde a definição dos cenários de ataque até a elaboração dos requisitos de informação do projeto, de troca e de informação do ativo. As etapas seguintes de desenvolvimento dos modelos em BIM e do add-on no Bonsai não foram elaboradas.

Como trabalhos futuros, sugere-se o desenvolvimento e a implementação do add-on no Bonsai seguindo este framework e o desenvolvimento de outros estudos de caso em edificações alvos, como subestações digitais de energia e torres de controle aéreo dado que são infraestruturas críticas. Outra funcionalidade interessante é a criação de uma interface de programação de aplicações (API) para permitir exportação dos dados para outros softwares.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

REFERÊNCIAS

AHN, Yong Han; CHO, Chung-Suk; LEE, Namhun. Building Information Modeling: Systematic Course Development for Undergraduate Construction Students. Journal of Professional Issues in Engineering Education and Practice, 2013, 139, 290–300.

ALVES, Josivan Leite; PALHA, Rachel Perez; ALMEIDA FILHO, Adiel Teixeira de. Investigação das aplicações integradas de inteligência artificial e BIM na indústria da construção civil. In: Simpósio Brasileiro de Tecnologia da Informação e Comunicação na Construção, 4., 2023, Porto Alegre. Porto Alegre: ANTAC, 2023. p. 1–12. DOI: 10.46421/sbtic.v4i00.2409.

CHEN, Si; XIANG, Dongming; JIN, Bo; JIN, Hua. Vulnerability assessment for physical protection systems of cave temples: A fuzzy petri net approach. Heliyon, 2024.

CÔRTES, Fernanda Laura dos Santos; MACIEL, Ana Carolina Fernandes. Estudo de interoperabilidade entre software BIM e softwares de análise energética de edificações (BES). In: Simpósio Brasileiro de Tecnologia da Informação e Comunicação na Construção, 3., 2021, Porto Alegre. Porto Alegre: ANTAC, 2021. p. 1–13. DOI: 10.46421/sbtic.v3i00.588.

CURSINO, Pedro Luis Soethe; MACHADO, Fernanda Almeida; SCHEER, Sergio. A interface GIS/BIM na mitigação de riscos de enchentes em áreas urbanas. In: Simpósio Brasileiro de Tecnologia da Informação e Comunicação na Construção, 3., 2021, Porto Alegre. Porto Alegre: ANTAC, 2021. p. 1–15. DOI: 10.46421/sbtic.v3i00.602. DONG, Mingxin; MENG, Yifei; SONG, Xiaomiao; QIN, Chuanrui; BAI, Mingqi; YIN, Fabo; ZHAO, Dongfeng. Research on vulnerability analysis model of security accident system in petrochemical enterprises. Process Safety Progress, 2021, 41. https://doi.org/10.1002/prs.12285.

DOS SANTOS, Eduardo RIBEIRO; SANTOS SALGADO, Mônica. ISO 19.650: uma reflexão sobre a importância da gestão e segurança da informação na indústria AEC. In: Simpósio Brasileiro de Qualidade de Projeto do Ambiente Construído, 7., 2021. Anais […]. [S. l.], 2021. p. 1–10. DOI: 10.29327/sbqp2021.437980.

DRESCH, Aline; LACERDA, Daniel Pacheco; ANTUNES, José Antonio Valle Júnior. Design Science Research: Método de Pesquisa para Avanço da Ciência e Tecnologia. Porto Alegre, Brasil: Bookman, 2015.

EBC, Agência Brasil, “Sumiço de metralhadoras é maior furto do Exército desde 2009”, disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2023-10/sumico-de-metralhadoras-e-maior-furto-do-exercito-desde-2009. Acesso em: 30 mar. 2025.

EKSTEDT, Mathias; JOHNSON, Pontus; LAGERSTRÖM, Robert; GORTON, Dan; NYDRÉN, Joakim; SHAHZAD, Khurram. Securi CAD by Foreseeti: A CAD Tool for Enterprise Cyber Security Management. In: 2015 IEEE 19th International Enterprise Distributed Object Computing Workshop, Adelaide, SA, Australia, 2015. p. 152–155. https://doi.org/10.1109/EDOCW.2015.40.

FORBES. Brazil is the world’s second most vulnerable country to cyberattacks. Disponível em: https://www.forbes.com/sites/angelicamarideoliveira/2023/09/27/brazil-is-the-worlds-second-most-vulnerable-country-to-cyberattacks/. Acesso em: 30 mar. 2025.

GALVÃO, Gabriel Andrade de Souza; CASTRO, Hiury Gandara de Toledo; COSTA, Bruno Rafael de Brito; MICELI JUNIOR, Giuseppe; PELLANDA, Paulo César. Aplicação de Gêmeos Digitais em um ambiente BIM de monitoramento de estruturas de edificações. In: Simpósio Brasileiro de Tecnologia da Informação e Comunicação na Construção, 4., 2023, Porto Alegre. Porto Alegre: ANTAC, 2023. p. 1–11. DOI: 10.46421/sbtic.v4i00.2590.

GODOI, T. C. Interoperabilidade entre Modelos BIM e Análises Energéticas: Desenvolvimento de Ferramenta no Blender para Integração de Dados de Modelos IFC Com Método Simplificado de Análise da INI-R. 133 p. Dissertação (Mestrado Profissional em Eficiência Energética e Sustentabilidade) — Fundação Universidade Federal de Mato Grosso do Sul, Mato Grosso do Sul, 2023.

ISO, BS EN ISO 19650-3: Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 3: Operational phase of the assets, 1ª ed, 2020.

ISO, BS EN ISO 19650-5: Organization and Digitization of Information about Buildings and Civil Engineering Works, Including Building Information Modelling (BIM) — Information Management Using Building Information Modelling — Part 5: Security Minded Approach to Information Management, 1ª ed, 2020.

LANGNER, Ralph. Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 2011, 9, 49–51. https://doi.org/10.1109/MSP.2011.67.

MARTINS, Ana Lucia Gallego; LIMA, Luana Souza Serafim de; SANTOS, Eduardo Toledo. O uso do BIM no canteiro de obras e a sua influência na segurança do trabalho. In: Simpósio Brasileiro de Tecnologia da Informação e Comunicação na Construção, 3., 2021, Porto Alegre. Porto Alegre: ANTAC, 2021. p. 1–12. DOI: 10.46421/sbtic.v3i00.615.

MESSNER, John; et al. (2019). Building Information Modeling Execution Planning Guide Version 2.2. The Pennsylvania State University.

MICELI JUNIOR, Giuseppe; PELLANDA, Paulo César; REIS, Marcelo de Miranda. Considerações sobre fluxos de trabalho BIM para desenvolvimento de projeto de obras em organizações públicas. In: Simpósio Brasileiro de Tecnologia da Informação e Comunicação na Construção, 2019, Campinas. Anais do 2º Simpósio Brasileiro de Tecnologia da Informação e Comunicação na Construção, 2019.

MICELI JUNIOR, Giuseppe; PELLANDA, Paulo César; REIS, Marcelo de Miranda. Modelagem da Informação da Construção para Gestão de Projetos de Obras de Infraestruturas de Defesa. Tese (Doutorado em Engenharia de Defesa) — Instituto Militar de Engenharia, Rio de Janeiro, 2019.

MOURA, Rebeca Viana Alencar Rodrigues; MICELI JUNIOR, Giuseppe; PELLANDA, Paulo César. Integração openBIM de modelo e orçamento com o sistema nacional de classificação de informação: uma proposta de fluxo de trabalho interoperável e colaborativo. Gestão & Tecnologia de Projetos, São Carlos, v. 19, n. 2, p. 261–283, 2024. DOI: 10.11606/gtp.v19i2.226681.

NEVES, Guilherme e SAUER, Frederico, “Segurança em redes: Como realizar análise de riscos de ameaças cibernéticas”, 1ª edição, Doutornet Tecnologia, 2014, 67p.

NIELSEN, Otto Araujo; MICELI JUNIOR, Giuseppe; PELLANDA, Paulo César. Contribuição para implementação BIM em organizações do setor de arquitetura, engenharia e construção. In: Simpósio Brasileiro de Tecnologia da Informação e Comunicação na Construção, 4., 2023, Porto Alegre. Porto Alegre: ANTAC, 2023. p. 1–9. DOI: 10.46421/sbtic.v4i00.2586.

NIELSEN, Otto Araujo; MICELI JUNIOR, Giuseppe; PELLANDA, Paulo César. Estudo da expansão de pesquisas em BIM a partir de palavras-chave: uma análise bibliométrica. In: Simpósio Brasileiro de Tecnologia da Informação e Comunicação na Construção, 4., 2023, Porto Alegre. Porto Alegre: ANTAC, 2023. p. 1–12. DOI: 10.46421/sbtic.v4i00.2587.

O GLOBO, “Polícia prende 6 em operação contra roubo de cargas; bando levou 10 mil balas de uma transportadora” disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/05/07/operacao-roubo-de-cargas-e-municao.ghtml Acesso em: 30 mar. 2025.

OTRANTO, Rafael Barbosa ; MICELI JUNIOR, Giuseppe ; PELLANDA, Paulo César . BIM-FM integration through openBIM: Solutions for interoperability towards efficient operations. Journal of Information Technology in Construction, v. 30, p. 298-318, 2025.

OLIVEIRA, J. A. Detecção de intrusão em sistemas industriais do setor elétrico: uma avaliação do uso de aprendizado de máquina e dos impactos de ataques. Dissertação (Mestrado em Engenharia de Defesa) — Instituto Militar de Engenharia, Rio de Janeiro, 2024.

PICCOLI, Débora Lins; TREBINO, Felipe Soares; NASCIMENTO, Natan Ramalho Lima; MELO, Reymard Savio Sampaio de; ALBERTE, Elaine Pinto Varela. Proposta de automatização de pagamento do concreto de paredes moldadas in loco integrando BIM e Blockchain. In: Simpósio Brasileiro de Tecnologia da Informação e Comunicação na Construção, 4., 2023, Porto Alegre. Porto Alegre: ANTAC, 2023. p. 1–12. DOI: 10.46421/sbtic.v4i00.2639.

PORTER, Stuart; TAN, Terence; TAN, Tele; WEST, Geoff. Breaking into BIM: performing static and dynamic security analysis with the aid of BIM. Automation in Construction, 2014, 40, 84–95. https://doi.org/10.1016/j.autcon.2013.12.002.

REFSDAL, A.; SOLHAUG, B.; STØLEN, K. (2015). Cybersecurity. In: Cyber-Risk Management. SpringerBriefs in Computer Science. Springer, Cham. https://doi.org/10.1007/978-3-319-23570-7_4.

REUTERS, “ Ukraine destroyed arsenal in Russia’s Tver region, Kyiv security source says” disponível em https://www.reuters.com/world/europe/ukraine-destroyed-arsenal-russias-tver-region-kyiv-security-source-says-2024-09-18/ Acesso em: 30 mar. 2025.

SUCCAR, B., Building Information Modelling Framework: A Research and Delivery Foundation for Industry Stakeholders. Automation in Construction, 2008, 18, 357-375.

SILVA, Gabriela Linhares da; GROETELAARS, Natalie Johanna. Uso de modelos BIM em realidade virtual e aumentada: panorama de aplicações e ferramentas. In: Simpósio Brasileiro de Tecnologia da Informação e Comunicação na Construção, 3., 2021, Porto Alegre. Porto Alegre: ANTAC, 2021. p. 1–13. DOI: 10.46421/sbtic.v3i00.565.

WERMANN, Alexandre Gustavo, BORTOLOZZO, Marcelo Cardoso. DA SILVA, Eduardo Germano , SCHAEFFER-FILHO, Alberto, GASPARY, Luciano Paschoal e BARCELLOS, Marinho, "ASTORIA: A framework for attack simulation and evaluation in smart grids," NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, Turkey, 2016, pp. 273-280, doi: 10.1109/NOMS.2016.7502822.