CONSIDERAÇÕES SOBRE O USO DE SALVAGUARDAS DE INFORMAÇÕES DIGITAIS PARA O PROJETO DE CONSTRUÇÕES DE USO SENSÍVEL EM BIM[1]

MICELI JUNIOR, M., Instituto Militar de Engenharia, e-mail: giuseppe.pged@ime.eb.br; PELLANDA, P. C., Instituto Militar de Engenharia, e-mail:pcpellanda@ieee.org; NASCIMENTO, A.F., Instituto Militar de Engenharia, e-mail: alexandrefitzner@gmail.com; TEIXEIRA, A. C., Instituto Militar de Engenharia, e-mail: acruz75@gmail.com

ABSTRACT

The increasing adoption of Building Information Modeling (BIM) in the management of Architecture, Engineering and Construction design processes has stimulated the intensification of digital information flow among project stakeholders. However, in the case where strategic and sensitive projects are being developed, such as military constructions, and support facilities for justice and public security, leakages and security breaches of sensitive data may compromise associated commercial objectives and intellectual property. This paper aims to bring to light some considerations about the use of digital information safeguards for the project of sensitive public activities in BIM, by adapting the standard PAS 1192-5: 2015 to the Brazilian reality.

***Keywords**: PAS1192-5. Building Information Modeling. Sensitive Assets.*

1 INTRODUÇÃO

O ambiente construído passa por um período de evolução e de mudança de paradigmas. A adoção do BIM (Building Information Modeling) e o crescente uso de tecnologias digitais terá um efeito marcante no projeto, construção e gestão de construções e de ativos. O aumento do emprego de plataformas colaborativas de trabalho, com a utilização de ambientes comuns de desenvolvimento (BSI,2013), contribuirá para uma intensificação do fluxo de informação digital entre os stakeholders de um projeto.

Como consequência desta tendência, é de se esperar, desde as primeiras fases do projeto, uma abordagem voltada à segurança dos dados de modelos de informação da construção. A primeira norma que trata desse assunto foi criada em 2015, a PAS 1192-5:2015 (*Specification for security-minded building information modelling, digital built environments and smart asset management*) com o objetivo de apresentar requisitos para o gerenciamento de projetos desenvolvidos em tecnologias digitais, com vistas à segurança da informação.

Este artigo trata de algumas considerações da aplicação dessa norma no projeto de construções governamentais que envolvem informações estratégicas e sensíveis cuja salvaguarda é um requisito desejável na

[1] MICELI JUNIOR, M. *et al*. Considerações sobre o uso de salvaguardas de informações digitais para o projeto de construções de uso sensível em BIM. In: ENCONTRO NACIONAL DE TECNOLOGIA DO AMBIENTE CONSTRUÍDO, 17., 2018, Foz do Iguaçu. **Anais**... Porto Alegre: ANTAC, 2018.

elaboração de projetos em plataformas BIM, como construções militares e instalações de apoio à justiça e à segurança pública no âmbito do Brasil.

2 SALVAGUARDA DE INFORMAÇÃO EM PROJETOS SENSÍVEIS

O British Standards Institute (BSI, 2015) define, em síntese, como ativos construídos sensíveis aquelas instalações que obedecem uma função diplomática, de segurança, de defesa nacional ou de aplicação da lei, bem como aqueles que foram julgados que pudessem ser utilizados para comprometer a integridade do ativo construído como um todo ou sua capacidade para funcionar.

Ainda de acordo com BSI (2015), os atributos específicos que devem ser considerados como sensíveis incluem, minimamente, a locação e os dados sobre:

- Sistemas de controle e vigilância;
- Maquinários permanentes;
- Detalhes estruturais de projeto;
- Salas de controle, acesso e segurança;
- Espaços regulados, ou que guardem substâncias ou informações reguladas;
- Especificações técnicas de produtos e características de segurança.

A salvaguarda a informações referentes a ativos sensíveis deve ser holística e envolver os três campos BIM definidos por Succar (2013) – tecnologias, pessoas e processos – e sobre eles, a dimensão de segurança física no que tange à segurança da informação.

BSI (2015) e NBS(2018) estabelecem uma sequência de atividades desde a intenção de se realizar o projeto, passando pela sua execução propriamente dita e acompanhando ainda a operação da construção.

As atividades geralmente começam com a realização, pelo empreendedor. de uma triagem de segurança para avaliação do nível de salvaguarda de informações que deve ser adotado, tanto com relação à construção do ativo como com relação aos ativos que lhe são vizinhos.

Deve ser ainda nomeado pelo empreendedor um gerente de segurança que será responsável por todo o assessoramento e acompanhamento dos procedimentos de segurança a serem desenvolvidos a partir daí.

A partir da concepção de um projeto considerado sensível, é necessário o levantamento detalhado dos seus requisitos de segurança junto ao contratante, para elaboração de uma Estratégia de Segurança do Ativo Construído (ESAC), que deve definir os procedimentos a serem empregados com respeito à manipulação, disseminação, armazenamento, acesso e uso de capturas seguras de todos os dados relativos a ativos e sistemas sensíveis. Isso pode incluir ainda a abordagem do fornecimento e intercâmbio de dados e informações com terceiros.

O avaliação dos riscos de segurança e a estratégia para dirimi-los devem estar contidos em uma estratégia de gerenciamento do risco do ambiente construído (EGRAC), que considera a avaliação dos riscos, das ações potenciais, das vulnerabilidades e dos impactos potenciais.

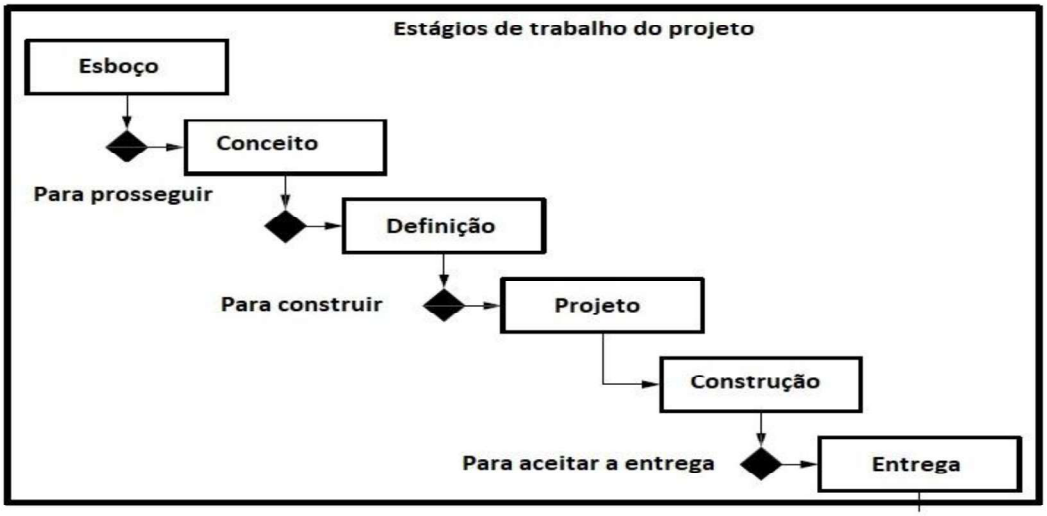
Devem ser previstas ainda as medidas para o gerenciamento dos incidentes e das violações de segurança que serão adotadas pelo gerente de segurança durante a construção e operação do ativo

Para que a Estratégia de Segurança do Ativo Construído (ESAC) seja seguida, é necessário detalhar a abordagem a ser tomada com a submissão de modelos e informações por meio de um Plano de Gerenciamento de Segurança do Ativo Construído (PGSAC).

Por outro lado, os Requisitos de Informações de Segurança do Ambiente Construído (RISAC) deve detalhar os requisitos do ativo com respeito aos arranjos para a captura segura, manuseio, disseminação, guarda, acesso e uso de todos os dados e informação relativas a ativos sensíveis e sistemas. Geralmente, as informações definidas nos RISAC serão contidas dentro do Plano de Execução BIM (PEB) e serão definidos pelo gerente de segurança em conjunto com o gerente de implantação BIM ou do projeto.

Entre uma fase da construção e outra os objetivos do projeto, a ESAC e todos os documentos anteriormente relacionados devem ser verificados e revisados, como exemplo mostrado na Figura 1.

Figura 1 – Marcos de revisão da estratégia de segurança



Fonte: BSI (2015), adaptado pelo autor

3 MODELO DE GESTÃO DO PROCESSO DE INSTALAÇÕES SENSÍVEIS

Para este trabalho, didaticamente a divisão do ciclo de vida do ambiente construído de uma obra pública foi dividida em cinco fases: planejamento, projeto, licitação, construção e operação.

A seguir, a partir de aplicações a uma construção pública voltada para utilização militar para utilização sensível, serão apresentados alguns pontos

que geralmente são constantes de uma ESAC e de seus documentos citados no item 2 deste trabalho.

3.1 Planejamento

A fase de planejamento abriga desde a decisão de se construir a instalação sensível, passando pelos estudos de viabilidade até a determinação para início do projeto. Nesta fase, o principal esforço deve ser de elaboração do ESAC e do PGSAC, que embasarão os requisitos de informações de segurança do ambiente construído (RISAC).

Toda a documentação deve ser analisada de forma que os requisitos sejam obedecidos nas fases seguintes do ciclo de vida do ativo, auxiliando na elaboração do PEB. A organização do arranjo de colaboração deve considerar que as informações considerados sensíveis (modelos, arquivos IFC ou mesmo planilhas do COBie) sejam separados dos não-sensíveis (BSI, 2015).

Igualmente, devem ficar definidas no PGSAC e reproduzidos no PEB as funções-chave do processo, que terão acesso integral aos planos de segurança supracitados e a todas as informações produzidas no âmbito do projeto. Todas as outras funções só terão acesso às informações necessárias para a execução do projeto.

Intercâmbios de informação com terceiros devem ser excluídos, ressalvando os contratados que assinam termo de compromisso de sigilo de informação no âmbito do projeto.

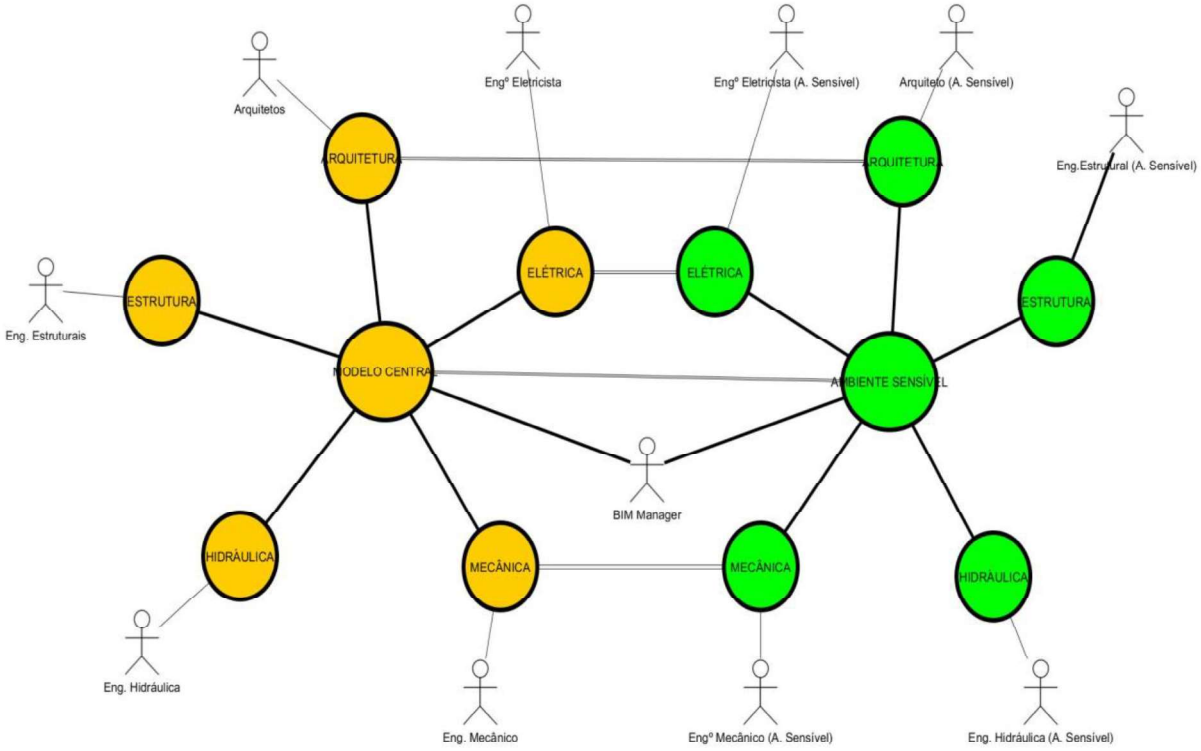
3.2 Projeto

Projeto envolve o processo de projeto propriamente dito. Deve-se garantir, nessa fase, o gerenciamento apropriado do detalhamento de informação, dos dados e dos modelos, de acordo com os RISAC no PEB.

A mesma importância que é dada ao treinamento na utilização dos *software* e no uso do ambiente de colaboração, deve ser dirigida à criação de uma mentalidade voltada para a salvaguarda de informações, não somente no âmbito dos modelos, mas inclusive nos relacionamentos interpessoais.

O empregador deve decidir e fazer constar nos PGSAC e no PEB a conveniência da separação de aspectos de projetos ou de projetos referentes à segurança. Se possível, deve ser criado um conjunto de *worksets* ou mesmo um novo modelo central somente para o ambiente sensível (conforme indicado em verde na Figura 2), com profissionais dedicados à modelagem de seus elementos mas em estreita comunicação com seus colegas.

Figura 2– Divisão possível dos worksets para projetos de áreas sensíveis



Fonte: autor

3.3 Licitação

Licitação envolve os esforços de contratação por parte do ente público da empresa que realizará a construção. Nesta altura do processo, apesar de já existir um modelo de construção com detalhamento alto (no mínimo ND 350), o planejamento das aquisições deve ser ligado ao sigilo dos sistemas e instalações que servem ao ativo.

Exemplificando, nunca a concorrência para a construção da obra civil (cujo sigilo se resume a descaracterizar alguns dados, como nas Figuras 3, 4 e 5), terá os mesmos requisitos de sigilo que os pregões para subcontratados especializados, onde não só o modelo ou os dados dele constantes mas principalmente o edital e o contrato terão que prever salvaguardas de proteção de informações operacionais de sistemas.

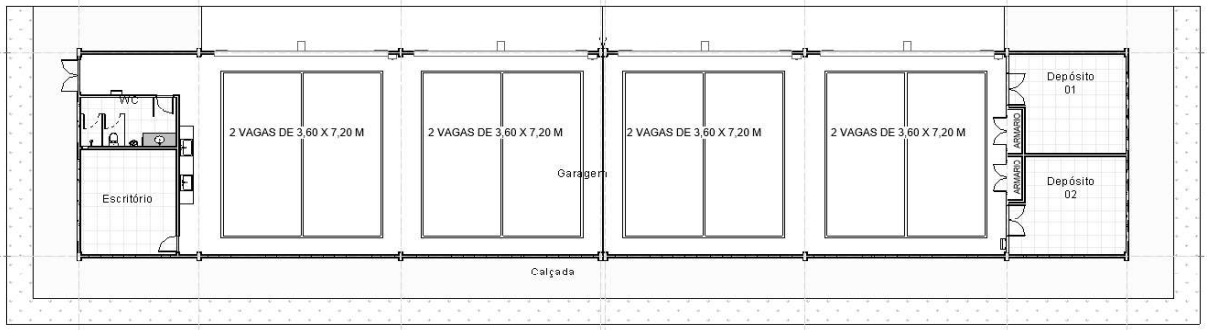
Além da proteção dos dados sensíveis, o contratante deve garantir, por meio de cláusulas editalícias contratuais (de confidencialidade e de requisitos de segurança) o correto manuseio e salvaguarda da informação. Informações de licitantes que não assinaram contrato com a Administração devem ser destruídas ou retornadas ao contratante.

Deve ser feito o possível para que os desenhos sejam disponibilizados em formatos como cópia impressa, imagens ou formatos PDF não interativos, ao invés de acesso a modelos que possam conter informações que não devam ser divulgadas.

Figura 3 – Descaracterização de ambientes em segundo piso de ativo

Fonte: adaptado pelo autor

Figura 4– Descaracterização de destinação de garagem

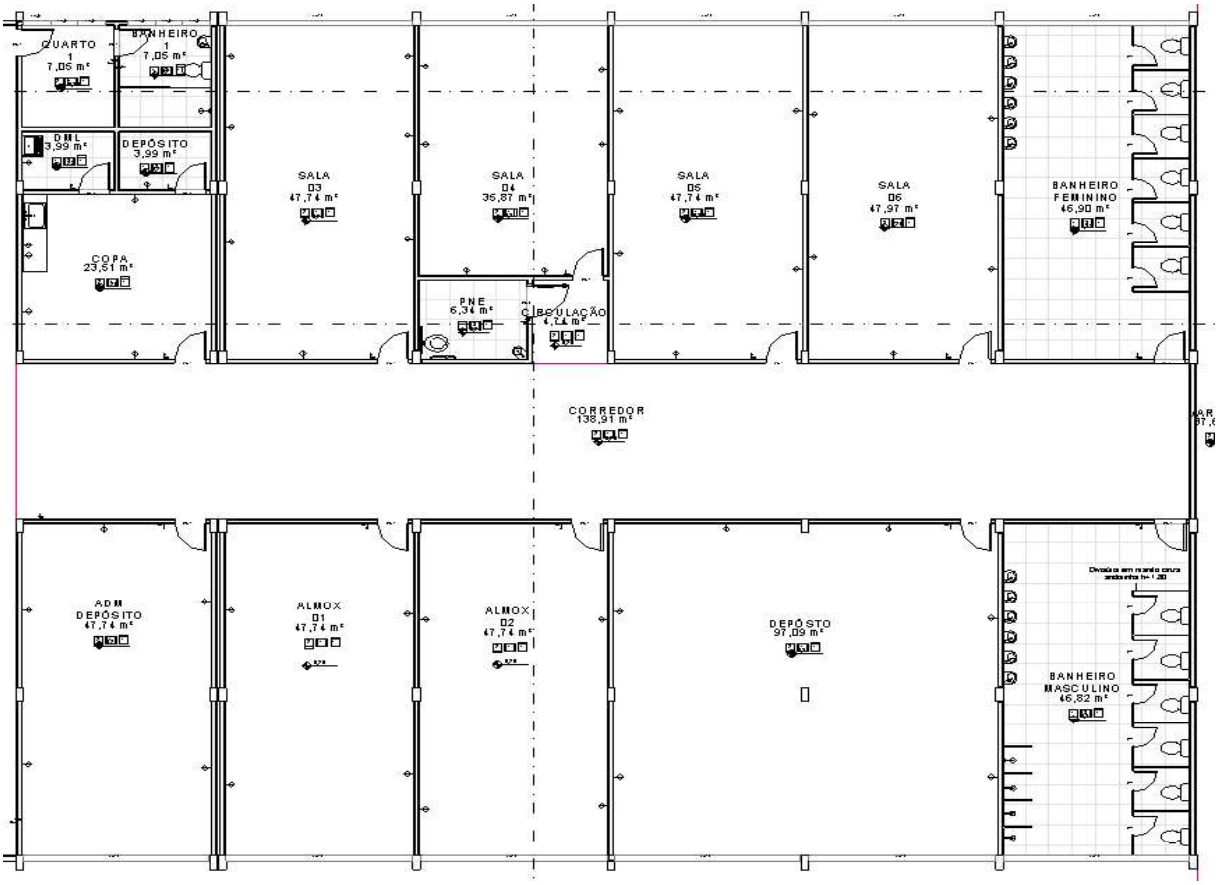


Fonte: adaptado pelo autor

3.4 Construção

Construção envolve os esforços de execução da obra por parte da empresa contratada e de sua fiscalização por parte do ente público. Nesta fase, deve-se confirmar como o canteiro de construção será gerenciado de forma segura, bem como atentar-se para os cuidados com os ativos e sistemas sensíveis a serem instaladas.

Figura 4 – Descaracterização de ambientes em primeiro piso de ativo



Fonte: adaptado pelo autor

Os cuidados com os modelos e os correspondentes arquivos devem ser intensificados, tendo em vista o aumento do fluxo de pessoas no canteiro e no escritório de projeto.

3.5 Operação

Inicia-se na entrega da obra ao cliente até seu descomissionamento, mudança de destinação ou demolição do ativo.

Deve-se preparar as informações para serem acrescentadas aos sistemas gerenciais da organização, a fim de integrar o modelo de informação do ativo. As medidas apropriadas para a salvaguarda destas novas informações devem ser aplicadas.

Todos os documentos referentes à obra devem ser avaliados; é salutar que documentos que tiverem como destino o descarte ou destruição devam ser arquivados pelo tempo previsto no plano de segurança ou em uma tabela de temporalidade de arquivos.

4 CONCLUSÕES

A adoção de modelos BIM em todas as etapas do ciclo de vida de uma construção propicia o aumento do fluxo de informações entre os *stakeholders* e em consequência o risco de vazamento de dados.

A adoção de uma mentalidade voltada para a proteção das informações de um modelo deve se refletir, como visto neste trabalho que se encontra em andamento, desde as etapas de planejamento da obra. Tais medidas especiais se refletem na adoção de medidas de triagem e de avaliação de risco de segurança e no estabelecimento de uma estratégia de segurança do ativo e de um plano de gerenciamento para sua execução.

Grande parte do que é estabelecido nessas medidas pode ser sintetizada no gerenciamento do acesso das informações somente necessárias para o trabalho de cada profissional e no gerenciamento contínuo da segurança da informação, desde a decisão pelo empreendimento até a mudança de destinação do ativo ou sua demolição.

Esclarece-se, contudo, que este trabalho está em andamento, com o desenvolvimento de um modelo de gestão dos aspectos referentes à ESAC e à salvaguarda de informações sensíveis em um projeto BIM.

REFERÊNCIAS

BSI BRITISH STANDARDS INSTITUTE**. PAS 1192-2:2013**: Specification for information management for the capital & delivery phase of construction using BIM. Reino Unido, 2013.

_____**. PAS 1192-5:2015**: Specification for security-minded building information modelling, digital built environments and smart asset management. Reino Unido, 2015.

DRESCH, A. *et al*. **Design Science Research**: método de pesquisa para avanço da ciência e tecnologia. 1. ed. São Paulo: Bookman, 2015.

NATIONAL BUILDING SPECIFICATION. **NBS BIM Toolkit** . Reino Unido: NBS, 2018. Disponível em: <https://toolkit.thenbs.com>. Acesso em: 20 jun. 2018.

SUCCAR, B. Building information modelling framework: A research and delivery foundation for industry stakeholders. **Automation in Construction**, Holanda, v. 18, n.3, maio 2009. p. 357-375. ISSN 0926-5805.