# GERENCIAMENTO DE RISCOS EM PROJETOS DE CASAS INTELIGENTES – SMART HOME

JEFERSON TADEU LIMA[1]

ANDRÉ PANHAM[2]

## RESUMO

Gestão de riscos é o processo de organizar e planejar recursos de forma a reduzir ao mínimo possível os impactos dos riscos na organização, utilizando um conjunto de técnicas que visam minimizar os efeitos dos danos, os processos de gerenciamento de riscos do projeto incluem os seguintes pontos: Planejar o Gerenciamento do Risco, Identificar os Riscos, Planejar Respostas aos Riscos e monitorá-los. O principal objetivo da Gestão de Riscos é avaliar as incertezas, possibilitando a melhor tomada de decisão possível. Nos projetos de casas inteligentes deve-se efetuar a gestão de risco de forma efetiva, podendo utilizar as técnicas definidas pelo PMBOK, pois dessa maneira poderá minimizar os impactos e as vulnerabilidades do projeto.O objetivo deste artigo é demonstrar a importância do gerenciamento dos riscos nas principais camadas do projeto de Casas Inteligentes: *Softwares*, dispositivos ou sensores de rede e atualização dos *Firmwares*.O sucesso de um projeto está diretamente relacionado com o esforço demandado nas etapas de Iniciação e Planejamento, quanto mais esforço for dedicado nestas etapas, maiores serão os indicadores de sucesso do projeto Casas Inteligentes.

**PALAVRAS-CHAVE**: Gestão de Riscos, Casas Inteligentes, Projetos.

[1] Graduado em Gestão de Tecnologia da Informação, FATEC, Câmpus Bragança Paulista, jtlima200@gmail.com
[2] Professor Doutor em Engenharia de Computação, IFSP, Câmpus Bragança Paulista, apanham@ifsp.edu.br

# *RISK MANAGEMENT IN SMART HOME PROJECTS*

## *ABSTRACT*

*Risk management is the process of organizing and verifying resources in order to minimize the risks of risks in the organization, using a set of techniques that aim to minimize the risks and risk management processes of the project. : Plan Risk, Identify Risks, Plan Responses to Risks and monitor them. The main objective of Risk Management is the possibility of decision making.In Smart Home projects, you must run a data generation software, which can be implemented as the techniques defined by the PMBOK, such as the vulnerabilities of the project. This article shows the marking of the main concepts of Smart Home design: Software, devices or sensors of network and update of the Firmwares. The success of a project is related to the effort required in the Initiation and Planning stages, the longer the earliest salary, the greater the success indicators of the Smart Home project.*

***KEYWORDS***: *Risk Management, Smart Home, Projects.*

## 1. INTRODUÇÃO

O gerenciamento de risco caminha com a humanidade desde a época do Renascentismo, período no qual as pessoas começaram a tomar suas decisões não mais baseadas em instintos ou crenças, pois começaram a ter embasamento em suas decisões, desde então não parou de evoluir, contribuindo com a sociedade em diversos segmentos e assim impulsionando a economia até os dias atuais. Podemos ver diversos exemplos dessa evolução, em vários nichos diferentes: o agricultor passou a produzir mais, de acordo com o resultado esperado versus o projetado, uma seguradora precifica o valor do seguro com base na avaliação do risco, um banco libera crédito para o correntista com base em uma análise de riscos, ou seja, podemos constatar que à gestão de risco no decorrer dos anos conquistou seu espaço, e no que diz respeito a gerenciamento de riscos em projetos de casas inteligentes não poderia ser diferente.

Tal evolução vem proporcionando ao longo dos anos a capacidade de definir o que poderá acontecer no futuro e tomar decisões mais assertivas sob condições de risco. Realizando uma análise da evolução do objetivo da gestão dos riscos, o PMBOK (2013) afirma que “[…] os objetivos do gerenciamento dos riscos do projeto são: aumentar a probabilidade e o impacto dos eventos positivos e reduzir a probabilidade e o impacto dos eventos negativos do projeto”.

Casas inteligentes é uma derivação da Internet das Coisas (IoT), este mercado está em plena expansão, mas ao mesmo tempo traz grandes desafios para as empresas. Uma pequena falha pode ocasionar grandes danos nas operações das organizações, e dependendo da proporção da falha e do porte da empresa, estes danos podem ser financeiros, legais, de reputação, entre outros (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2010).

A ideia de automatizar uma residência, torná-la inteligente, define-se em simplificar e facilitar diversas ações realizadas no dia-a-dia, tanto para pessoas comuns como também para pessoas com deficiência, que não podem se locomover para abrir uma janela ou uma porta, acionar uma torneira, ou qualquer outro tipo de ação que venha para facilitar.

A variedade de dispositivos que podem ser instalados em uma residência é enorme e a cada dia são lançados novos produtos e serviços. Os dispositivos mais

comuns apresentados para tal finalidade no momento são: sistema de iluminação controlável, condicionador de ar com atuação customizada, acionamento do portão eletrônico, sensores e alarmes. Dessa gama de produtos inovadores lançados diariamente no mercado, podemos citar que os sistemas de monitoramento e segurança são os que mais evoluem.

O foco deste artigo é o gerenciamento de riscos em projetos de Casas Inteligentes, a casa inteligente está online 24 horas por dia, 7 dias por semana, devido a essa exposição de transação de dados na internet, a casa inteligente está vulnerável a atacantes maldosos que podem tentar acessá-la com a intenção de roubar ou sequestrar dados dos usuários interligados nessa rede. Além dos riscos de conectividades, outros riscos como softwares embarcados e sensores de Iot, também correlacionados a projetos de casas inteligentes estarão descritos no decorrer deste artigo.

Um projeto bem estruturado de Casa Inteligente busca minimizar os riscos das falhas de exposição dos dados em suas transações. Essas falhas podem ocorrer como consequência do não gerenciamento dos riscos presentes no âmbito deste projeto.

Projeto é um esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo, que utiliza recursos limitados, conduzido por pessoas visando atingir metas e objetivos pré-definidos e estabelecidos dentro de parâmetros de prazo, custo e qualidade (PMI, 2008).

Segundo Kendrick (2003 *apud*, NEVES e SILVA, 2016) “todos os projetos apresentam riscos, mas projetos de alta tecnologia apresentam riscos particulares, como alta variação”.

Buscando proporcionar uma maior familiaridade com o gerenciamento de riscos em projetos de Casas Inteligentes foi realizada uma pesquisa exploratória baseada em pesquisa bibliográfica e estudo de caso. O principal objetivo desta pesquisa é levantar informações sobre gerenciamento de riscos em projetos de casas inteligentes, analisando as possíveis vulnerabilidades em nível de sistemas (*softwares*), conectividade na rede, dispositivos e sensores.

Este artigo está organizado em três partes. A primeira parte foi o levantamento de material de pesquisa, buscando o que há de mais novo referente aos riscos e as principais vulnerabilidades encontradas em um ambiente de rede. Após este

levantamento, foram relacionadas todas as fases de um projeto com os dispositivos pertencentes a uma rede IoT dentro de uma casa inteligente. Além disso, foi realizada uma busca por possíveis riscos e vulnerabilidades no desenvolvimento de um *software* de um projeto de uma casa inteligente, tendo como objetivo encontrar abordagens mais adequadas sobre este novo cenário de casas inteligentes. A Segunda parte foi elaborar uma tabela ressaltando e resumindo os principais riscos no gerenciamento de um projeto de casa inteligente, juntamente comas principais vulnerabilidades encontradas durante a pesquisa. Terceira e última parte é a conclusão deste artigo que propõe expor as análises, dando embasamento para obras e pesquisas futuras.

## 2. FUNDAMENTAÇÃO TEÓRICA

O termo risco é originado do latim *risicu* ou *riscu*, que significa ousar, proveniente de um pensamento embasado em algo negativo ou que pode não dar certo, porém, atualmente esta visão foi remodelada com a inclusão da qualificação e da quantificação dos riscos e os possíveis ganhos ou perdas em um planejamento tanto em âmbito profissional quanto pessoal (ABRAHAM, 2012 *apud* SCOFANO, 2013). Com base nessa definição, no cenário de um projeto de *software* complexo, percebemos que suportar um risco pode ser algo positivo desde que se faça com um bom planejamento, mapeando o quanto os envolvidos podem suportar algo negativo e lidar com suas expectativas para alcançar uma oportunidade no futuro.

Um dos maiores desafios da gestão de riscos é lidar com a expectativa frente ao risco e para Baraldi (2010 *apud* SCOFANO, 2013), o risco é definido como elementos incertos às expectativas, aquilo que age constantemente sobre os objetivos, as metas e os meios estratégicos (pessoas, processos, informação e comunicação), influenciando o ambiente e podendo trazer prejuízos. Nascimento (2003) salienta que as incertezas podem contribuir diretamente para o risco de um projeto. No entanto, os riscos quando bem gerenciados, podem criar oportunidades de ganhos e de formas de melhoria (GAEA, 2017).

Ignorar o gerenciamento dos riscos frequentemente resulta em consequências indesejáveis, que vão desde requisitos não atendidos, perdas financeiras e problemas

de desempenho, até ao completo fracasso do projeto (WALLACE; KEIL 2004 apud CÂMARA et al., 2015).

O termo domótica é originado da junção das palavras Domus, que em latim significa casa, e robótica, que representa uma tecnologia capaz de controlar todos os ambientes de uma residência através de um só equipamento, incluindo temperatura, luminosidade, som, segurança, dentre outros, ou seja, automação residencial (BOLZANI, 2004; FERREIRA, 2008; SGARBI , 2007).

Segundo Brugnera (2008), “a domótica é um recurso utilizado para controle de um ou mais aparelhos eletrônicos por meio de uma central computadorizada”.

Domótica é um processo ou sistema que prioriza a melhoria do estilo de vida (das pessoas), do conforto, da segurança e da economia da residência, através de um controle centralizado das funções desta, como água, luz, telefone e sistemas de segurança, entre outros (ANGEL, 1993 e NUNES, 2002). Para corresponder as exigências, a domótica faz uso de vários equipamentos distribuídos pela residência de acordo com as necessidades dos moradores. Estes equipamentos podem ser divididos em três principais grupos (TAKIUCHI et al, 2004): Atuadores: controlam os aparelhos da residência como, por exemplo, luz e ventilador, Sensores: capturam informações do ambiente como, por exemplo, luminosidade, umidade e presença, Controladores: são responsáveis pela administração dos atuadores e sensores, ou seja, coordenam todos os aparelhos e equipamentos da residência que fazem parte da automação.

## 3. CONTEXTUALIZAÇÃO E DESENVOLVIMENTO

Os riscos de uma Casa Inteligente estão relacionados às tecnologias que são escolhidas para o desenvolvimento do projeto. Pode-se entender que o desenvolvimento de uma Casa Inteligente está baseado no uso intenso de novas tecnologias como: Redes de Sensores, IoT, Computação em Nuvem e Big Data.

Desta forma, os riscos de um projeto de Casa Inteligente estão relacionados basicamente em explorar as vulnerabilidades de dispositivos mal projetados, que podem expor os dados do usuário de maneira desnecessária.

Assim, neste artigo houve a concentração dos esforços nos seguintes riscos ou vulnerabilidades:

- O *Software*:
  - Os dispositivos inteligentes que serão instalados na casa, terão *softwares* embarcados.
  - *Softwares* mal projetados poderão causar falhas de segurança.
  - Testes de segurança são uma maneira de encontrar vulnerabilidades de segurança no *software* e minimizar os riscos.

- A conectividade na rede:
  - A Casa Inteligente permanecerá conectada 24 horas por dia.
  - Os códigos desenvolvidos nos dispositivos, sem a segurança apropriada deixará a conectividade vulnerável.
  - Uma das principais causas dessa vulnerabilidade, é devido à muitos dos engenheiros encarregados da concepção e na construção das soluções, não serem especialistas em protocolos de rede e em segurança das mesmas.

- As atualizações de *firmwares*:
  - A grande maioria dos dispositivos instalados nas casas não requer regulamentação.
  - As atualizações não são fornecidas frequentemente e automaticamente pelos fabricantes.
  - A falta de atualizações de *firmwares* resulta em vulnerabilidade de segurança, permitindo ataques maldosos e possibilitando o controle completo do dispositivo.

- Os sistemas promíscuos:
  - Os ataques direcionados a centros de dados são uma estratégia utilizada frequentemente pelos atacantes maldosos.
  - Agindo no dispositivo pelo *download* de um *malware* e se movimentando pela rede até encontrar o banco de dados completo de IPs sensíveis ou informações do cliente.

Seguem alguns aspectos que foram abordados no decorrer deste artigo:

- Boas práticas de projeto;
- Custo versus Segurança;
- Padrões e Métricas;
- Confidencialidade dos Dados, Autenticação e Controle de Acesso;
- Capacidade de Atualização;
- Responsabilidade Compartilhada;
- Regulamentação;
- Obsolescência de dispositivos;

Todas as vulnerabilidades citadas acima, caso não tenham o tratamento adequado podem trazer riscos a um projeto de Casa Inteligente.

Ao analisar os dados expostos nesta seção do artigo, pode-se verificar que o risco está implícito em todas as fases desse projeto, desde a escolha dos dispositivos e sensores, até a definição do serviço de *Cloud Computing* adequado, juntamente com as atualizações dos *Firmwares* e protocolos de segurança a serem utilizados.

Enfim, pode-se afirmar que este tipo de projeto possui alta vulnerabilidade, pois mantém diversas janelas de acessos que permitem a um atacante ingressar e fazer um mau uso das informações e dados trafegados nesse ambiente. No decorrer deste artigo, buscou-se expor as principais maneiras de se prevenir e remediar tais situações, baseando-se em 3 frentes para o gerenciamento dos riscos: *Software*, dispositivos de rede e *firmwares*.

## 3. 1 PLANEJAR O GERENCIAMENTO DOS RISCOS

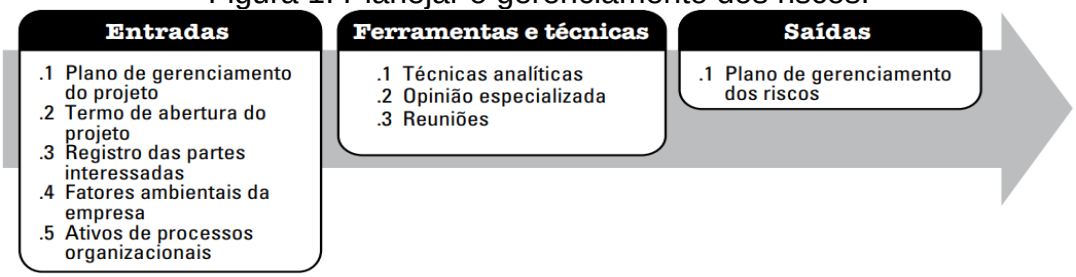
Com relação a gerenciamento de riscos esta é a etapa inicial do processo, pois é nesse momento que se deve garantir que todo processo de planejamento dos riscos seja executado de maneira efetiva.

Essa fase inicial do gerenciamento de riscos, focou-se em 3 frentes para o gerenciamento dos riscos: *Softwares*, dispositivos de rede e *firmwares*.

Segundo Linhares e Quartaroli (2004) *apud* Palma *et al*. (2011), nesta etapa “deve-se desenvolver, documentar e organizar a estratégia de riscos, estabelecendo propósitos e objetivos, definindo responsabilidades para áreas específicas,

identificando técnicas e expertises adicionais, estabelecendo métricas, definindo relatórios e documentação", é possível verificar tal ilustração na figura 1.

Figura 1. Planejar o gerenciamento dos riscos.




Fonte: PMI (2013, p.313).

Segundo PMI (2013), opiniões de especialistas, reuniões e técnicas analíticas que tem como objetivo classificar e qualificar seu apetite de risco e tolerância por meio de uma análise de perfil de riscos das partes interessadas.

Relacionando essa análise do PMI com a realidade deste projeto, pode-se afirmar que as partes interessadas citadas no parágrafo anterior, podem ser simbolizadas como a relação entre o *Software*, juntamente com os dispositivos de rede, que também são chamados de sensores ou atuadores, nos projetos de IoT.

Seguem alguns exemplos destes dispositivos IoT, voltados para Casa Inteligentes: Sensores de temperatura e umidade, Sensores de luminosidade, Sensores de presença, dispositivos controlados por tempo, relês atuadores, acionadores automatizados e motores e servo motores.

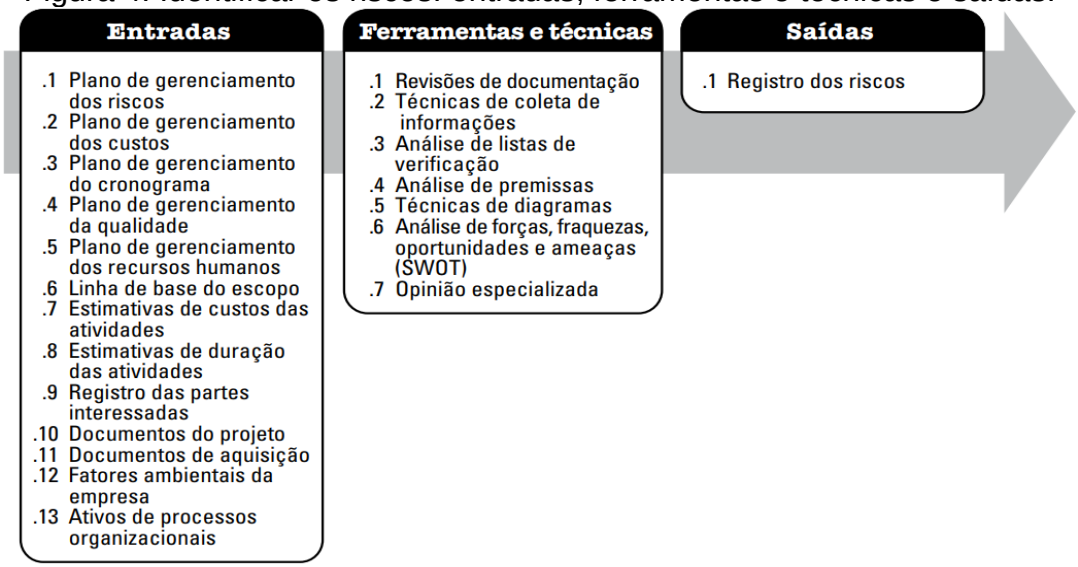
## 3.2 IDENTIFICAR OS RISCOS

Com base em uma pesquisa que possua embasamento e argumentações de especialistas, pode-se identificar os principais riscos que podem afetar o projeto de uma Casa Inteligente. Devem-se sumarizar os resultados desta pesquisa e evidenciá-las em uma base de conhecimento, colocando o máximo de informações e buscando caracterizar os tipos de ameaças, tendo como objetivo principal se antecipar aos eventos e vulnerabilidades.

O resultado do processo de identificar os riscos é obtido com a entrada do plano de gerenciamento de risco obtido por meio da saída do fluxo da Figura 1. Ou seja, de acordo com as ilustrações do PMI, as entradas e saídas de um fluxo sempre serão

concomitantes, conforme demonstrado a seguir na figura 4.

Figura 4. Identificar os riscos: entradas, ferramentas e técnicas e saídas.




Fonte: PMI (2013, p.319).

Segundo o PMI (2013), “identificar os riscos é o processo de determinação dos riscos que podem afetar o projeto e de documentação de suas características”.

Cabe salientar que o Plano de Gerenciamento de Riscos não tem um caráter estático e deve ser frequentemente alterado e ajustado de acordo com os avanços do projeto, porém, em projetos menores e de baixo custo, ou de baixo risco, este plano não é requerido em sua totalidade (COOPER *et al*., 2005).

Para projetos de Casas Inteligentes, deve-se haver uma documentação inicial, na qual contenha os principais riscos identificados e suas prováveis tratativas, de acordo com a complexidade de cada uma das vulnerabilidades. Essa documentação deve ser atualizada sempre que necessário, pois as vulnerabilidades não são estáticas e estão em constantes evoluções. Como exemplo, pode-se afirmar as crescentes disseminações de vírus, *trojans* e *malwares* espalhados pelas redes e dispositivos periféricos.

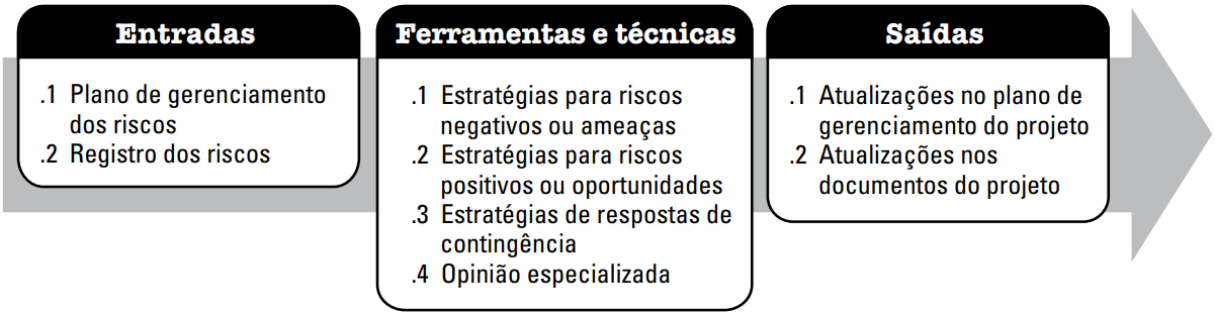
## 3.3 PLANEJAR RESPOSTAS AOS RISCOS

Para cada um dos riscos identificados no capítulo anterior, deve-se desenvolver planos de ações para aumentar as oportunidades e reduzir as ameaças aos objetivos

do projeto, este processo inicia-se com a entradas obtidas por meio das saídas da Figuras 1 e 4, conforme observa-se na Figura 5. De acordo com Kerzner (2011, p. 483):

> O planejamento de respostas aos riscos deve ser compatível com o plano de gerenciamento de riscos e com qualquer orientação adicional que o gerente de programa forneça. Uma parte crítica do planejamento das respostas aos riscos envolve o refinamento e a seleção da resposta mais adequada e abordagens específicas de aplicação para os riscos e oportunidades selecionados.

Figura 5. Planejar as respostas aos riscos: entradas, ferramentas e técnicas e saídas.




Fonte: PMI (2013, p.342).

Dando embasamento ao exposto pelo PMI, em projetos de casas inteligentes é possível prever e anteceder algumas possíveis vulnerabilidades e descrever consequentemente algumas respostas aos riscos identificados. Como exemplo, foi citado na seção de contextualização a questão a atualização dos *Firmwares*, ou seja, o risco identificado nessa situação é a baixa taxa de *patches* de atualização de *firmwares*, sendo assim, é possível planejar uma resposta a esse risco identificado, pois, buscando equipamentos que tenha comprometimento com a qualidade e segurança de seus dispositivos e emitam *patches* de segurança de *Firmwares* com demasiada frequência.

## 3.4 CONTROLAR OS RISCOS

Controlar os riscos é uma etapa do projeto que pertence a fase denominada de processo de monitoramento e controle, onde é possível avaliar de forma sistêmica e eficaz as ações de resposta aos riscos, em relação às métricas estabelecidas. Assim como os passos anteriores, essa etapa se inicia com a entrada das informações obtidas por meio das saídas das Figuras 1, 4 e 5. As informações obtidas durante os

processos anteriores servem de base para formular novas estratégias de resposta ao risco, bem como o aprimoramento das estratégias atuais. O foco é estabelecer indicadores de gestão de custo, desempenho, e cronograma do programa para que todos os interessados possam avaliar o andamento do mesmo (KERZNER, 2011).

Na figura 6 podemos identificar a continuidade do fluxo de gerenciamento dos riscos e todas as suas derivações:

Figura 6. Controlar os riscos: entradas, ferramentas e técnicas, e saídas.


Fonte: PMI (2013, p.349).

Controlar os riscos em um projeto de Casa Inteligente está diretamente interligado com o exemplo citado na contextualização deste artigo, principalmente na parte onde citou-se a relação dos dispositivos de segurança possuírem *softwares* embarcados de baixa qualidade de segurança e grandes vulnerabilidades, esse tipo de risco pode ser controlado desde que haja o devido mapeamento de suas identificações e suas respostas devidamente planejadas, assim como a atualização dos *firmwares* citados no capítulo anterior.

Para maior controle e monitoramento dos riscos é necessário que as etapas que antecedem este processo tenham sido incessantemente questionadas e debatidas, pois assim o gerente do projeto da Casa Inteligente terá argumentos e um grande arcabouço teórico sobre o assunto.

## 4. ANÁLISE DAS VULNERABILIDADES

As análises das vulnerabilidades foram divididas em 3 tópicos que foram o ponto focal do estudo elaborado nesse artigo, pois os principais riscos em projetos de Casas Inteligentes estão diretamente relacionados aos três tópicos abaixo: *Software*, Dispositivos ou Sensores e por último os *Firmwares.*

### *4.1 Software*

A maioria dos dispositivos e sensores de redes geralmente possui um baixo poder de processamento, para isso os mesmos possuem *softwares* embarcados, em muitas das vezes estes *softwares* são desenvolvidos sem a devida atenção nas questões voltadas para protocolos de segurança, dessa forma, poderão vir a proporcionar falhas de segurança e apresentar uma vulnerabilidade de acesso a sua rede de navegação.

Uma das maneiras de minimizar riscos e vulnerabilidades de segurança nos *softwares* embarcados é a utilização de testes unitários e massivos de segurança, utilizarem testes automatizados para ataques de segurança, pode ser uma forma de minimizar a exposição aos malfeitores.

Um sistema embarcado é um sistema no qual o computador é completamente dedicado ao dispositivo ou sistema que ele controla. Um sistema embarcado realiza um conjunto de tarefas predefinidas, geralmente com requisitos específicos. Tratando-se de tarefas específicas, pode-se otimizar o projeto reduzindo tamanho, recursos computacionais e custo do produto.

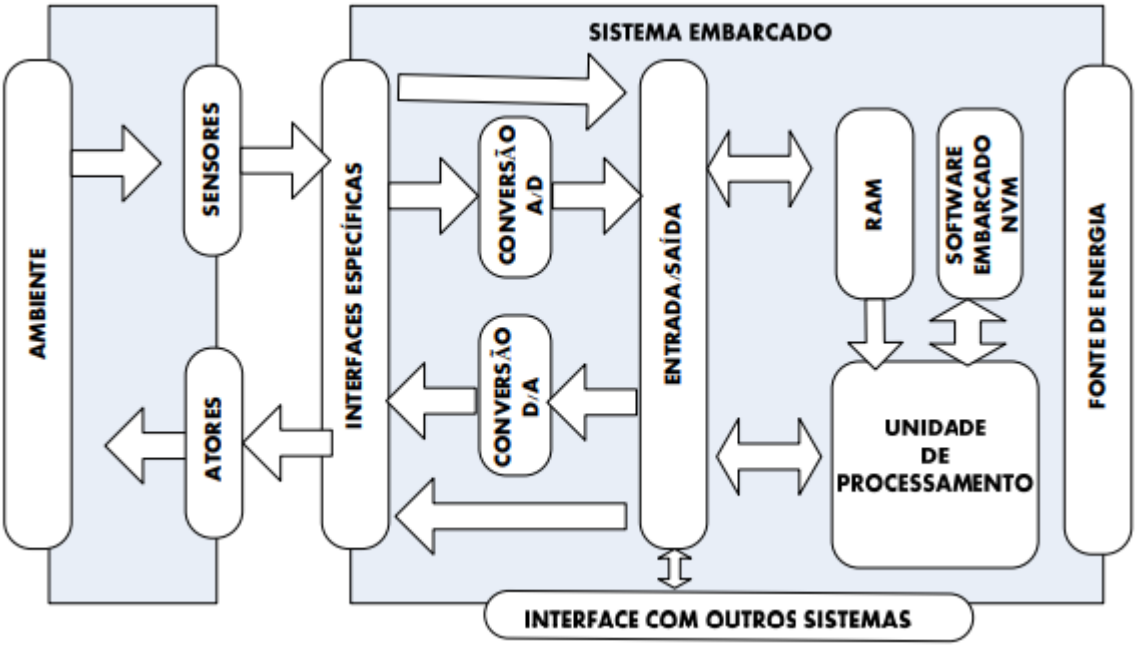
No decorrer deste capítulo consta a Figura 6, a qual apresenta um esquema genérico de um sistema embarcado. Segue também a Tabela 1, onde consta a análise das vulnerabilidades de softwares embarcados.

Tabela 1 - Análise das Vulnerabilidades dos Softwares Embarcados

| **Análise das Vulnerabilidades dos Softwares** | | | | |
|---|---|---|---|---|
| | **Planejar** | **Identificar** | **Respostas** | **Controlar** |
| **Boas práticas de projeto de software embarcado** | 1.Definir a Linguagem de Programação;<br><br>2.Programar com embasamento em convenções; | 1.Risco de escolher uma linguagem obsoleta;<br><br>2.Risco de escolher uma convenção desconhecida pela equipe DEV; | 1.Ter uma segunda opção de linguagem de programação na qual a equipe DEV tenha conhecimento.<br><br>2.Determinar um padrão de desenvolvimento ou uma convenção, na qual todos os | 1.Monitorar a equipe de desenvolvimento e atualizar o conhecimento.<br><br>2.Controlar a qualidade das linhas de código digitadas e não somente o resultado entregue. |

| | | | | |
|---|---|---|---|---|
| | | | DEVs tenham domínio. | |
| **Padrões e Métricas** | 3.Programar em Camadas; | 3.Risco de não delimitar as fronteiras (integrações) de desenvolvimento; | 3.Elaboração de uma Especificação técnica irá minimizar os riscos. | 3.Comparar o desenvolvimento com a documentação técnica e gerar evidencias para embasar o monitoramento. |
| **Obsolescência de dispositivos** | 4.Escolher um dispositivo adequado para o desenvolvimento. | 4.Pesquisar se o dispositivo escolhido possui continuidade no mercado. | 4.Caso o mesmo tenha um ciclo de vida curto ou indefinido, o mesmo deverá ser substituindo por um moderno. | 4.Monitorar a vida útil dos dispositivos e seus upgrades. |
| **Capacidade de Atualização** | 5.Escolher um dispositivo que possua um reconhecimento de mercado. | 5.Identificar as prováveis falhas passadas relacionadas a atualização de softwares da mesma marca. | 5.Substituí-lo por equipamentos que atendam os padrões mínimos determinados no projeto. | 5.Mantê-lo atualizado e monitorá-lo para acompanhar seu ciclo de vida e utilização. |
| **Confidencialidade dos Dados, Autenticação e Controle de Acesso** | 6.Planejar a utilização de protocolos de segurança com maturidade e bem avaliado no cenário de T.I. | 6.Identificar quais os protocolos estão sendo utilizados no momento do desenvolvimento do software embarcado. | 6.Ter uma segunda opção que atenda requisitos mínimos de segurança descritos no projeto. | 6.Controlar a segurança através de testes massivos e direcionados a aplicação. |

Figura 6 - Esquema genérico de um sistema embarcado




Fonte:Broekman e Notenboom, 2002

### 4.2. Sensores e dispositivos de Rede

A Casa Inteligente estará conectada através de sensores e dispositivos ligados a internet 24 horas por dia, 7 dias por semana, ou seja, a mesma estará online e deverá seguir a regra dos pilares da segurança em T.I.: Confidencialidade, integridade e disponibilidade.

Todas com suas devidas responsabilidades, não havendo uma mais prioritária que a outra:

1. **Confidencialidade:** Este conceito tem relação com a privacidade dos dados trafegados dentro de uma rede.
2. **Integridade:** Corresponde a preservação da precisão dos dados em uma rede, tais dados devem ser íntegros, sem interferências externas, para não causar dupla interpretação, pois isso impactará no poder de tomada de decisão.
3. **Disponibilidade:** trata-se da disposição dos dados a qualquer instante, podendo ser avessado de qualquer lugar, ou seja, o mesmo deve estar disponível ao usuário a qualquer momento que o mesmo solicitar.

Na tabela 2 apresentada na sequência deste capítulo, podemos observar uma análise das vulnerabilidades dos sensores e dispositivos de rede que podem ser utilizados em um projeto de Casa Inteligente.

Tabela 2 - Análise das Vulnerabilidades dos Sensores e Dispositivos de rede

| **Análise das Vulnerabilidades dos Sensores e Dispositivos de rede** | | | | |
|---|---|---|---|---|
| | **Planejar** | **Identificar** | **Respostas** | **Controlar** |
| **Confidencialidade dos Dados, Autenticação e Controle de Acesso** | 1.Planejar a utilização de protocolos de segurança com maturidade e bem avaliado no cenário de T.I. | 1.Identificar quais os protocolos estão sendo utilizados no momento do desenvolvimento do software embarcado. | 1.Ter uma segunda opção que atenda requisitos mínimos de segurança descritos no projeto. | 1.Controlar a segurança através de testes massivos e direcionados a aplicação. |
| **Integridade dos dados** | 2. Escolher sensores e dispositivos que entreguem os pacotes com integridade | 2.Identificar prováveis perdas de pacotes de dados transacionados entre o dispositivo e a central de comando. | 2.Elaborar necessidades que atendem a provável perda de pacote, traçar rotas pré-definidas para comunicação dos equipamentos entre gateway. | 2. Monitorar a totalidade dos dados transacionados e as prováveis perdas, pois assim poderá minimizar as mesmas. |
| **Obsolescência de dispositivos** | 3. A escolha adequada dos dispositivos e sensores deverão seguir requisitos técnicos que atendam a necessidade do cliente | 3. Identificar prováveis dispositivos e sensores alocados na rede que possuam resquícios de obsolescência. | 3. Ter em mãos equipamentos que em caso de falha possam vir a substituir o sensor obsoleto e a necessidade do projeto. | 3. Através do monitoramento será possível trabalhar com prevenção as falhas. |
| **Disponibilidade dos dados** | 4. Os dispositivos e sensores devem estar disponível na rede assim que configurados e podem ser acessados a qualquer momento. | 4.Através de uma configuração de rede adequada é possível customizar a rede para que o dispositivo esteja enviando status a todo instante. | 4. Em caso de falha na disponibilidade de dados de um sensor ou dispositivo, o mesmo deverá ser levado a uma banca de testes para validar seu funcionamento. | 4.O ato de controlar ou monitorar um sensor ou dispositivo de rede, deve ser feito através de comandos de validações. |

### *4.3. Firmwares*

A grande maioria dos dispositivos instalados nas casas não requer regulamentações, por isso a maioria das empresas fabricantes destes sensores ou

dispositivos não fornecem frequentemente e automaticamente atualizações de seus *firmwares*. Essa falta de atualização dos *Firmwares* resulta em vulnerabilidade de segurança, permitindo ataques maldosos e possibilitando o controle completo do dispositivo, ou até mesmo de outros dispositivos dentro da mesma rede. Através dessa vulnerabilidade de *Firmware,* atacantes maldosos podem agir no dispositivo através do *download* de um *malware* e transitar pela rede até encontrar o banco de dados completo de IPs sensíveis ou informações sobre cliente. Dando continuidade nas análises das vulnerabilidades dos Firmwares, na tabela 3 pode-se observar os principais pontos críticos relacionados aos Firmwares.

Tabela 3 - Análise das Vulnerabilidades dos Firmwares

| **Análise das Vulnerabilidades dos Firmwares** | | | | |
|---|---|---|---|---|
| | **Planejar** | **Identificar** | **Respostas** | **Controlar** |
| **Autenticação e Controle de Acesso** | 1.Planejar a utilização de protocolos de segurança para autenticação e edição através de controles de acesso. | 1.Identificar quais os protocolos estão sendo utilizados no momento do desenvolvimento do Firmware e suas prováveis vulnerabilidades. | 1.Buscar uma segunda opção que atenda requisitos técnicos de segurança de software, essa alternativa tem que estar disponível a qualquer instante para utilização. | 1.Controlar a segurança através de testes massivos e direcionados a aplicação. |
| **Padrões e métricas** | 2. Manter um padrão de desenvolvimento dentro de uma linguagem de programação de conhecimento da equipe de desenvolvimento. | 2.Identificar prováveis desvios de condutas e padrões de desenvolvimento. | 2.Elaborar respostas que atendam a necessidades de padronização para os desenvolvedores que não estão seguindo a cartilha de desenvolvimento. | 2. Monitorar através de softwares especializados, se os padrões de desenvolvimentos estão sendo seguidos pelas equipes. |
| **Obsolescência da codificação** | 3. Escolha adequada da linguagem de Programação que atenda a necessidade do Firmware, minimizando as vulnerabilidades. | 3. Identificar prováveis pontos de obsolescência na arquitetura do Firmware e de sua estrutura de códigos. | 3. Buscar uma segunda opção de desenvolvimento arquitetural de software com opção de atualização tecnológica, através de frameworks e bibliotecas de segurança já | 3. Monitorar o ciclo de vida útil da arquitetura desenvolvida sob o firmware e atentar as novas ameaças disponíveis, mantendo atualizado seu repositório de patches de segurança. |

| | | | | |
|---|---|---|---|---|
| | | | disponíveis no mercado. | |
| **Capacidade de Atualização** | 4. Escolher um dispositivo que possua um fabricante de mercado que tenha como prática a atualização de seus firmwares. | 4. Identificar as prováveis falhas relacionadas a atualização de patches segurança. | 4. Manter uma validação de versionamento no firmware do equipamento, buscando atender padrões técnicos adequados. | 4. Manter a atualização e o versionamento para monitorar seu ciclo de vida e utilização. |
| **Responsabilidade compartilhada** | 5. Escolher dispositivos e sensores que busquem atender os requisitos técnicos juntamente com a necessidade da solução. | 5. Identificar prováveis pontos vulneráveis dentro da rede de dispositivos e sensores alocados. | 5. Investir em equipamentos renomados que tenham a responsabilidade compartilhada e busquem minimizar falhas de segurança. | 5. Através do monitoramento da versão dos firmwares instalados, é possível trabalhar com prevenção as falhas e vigorando dentro das normas da legislação. |

## 5. CONCLUSÕES

Este artigo apresentou uma análise de como o gerenciamento de risco em projetos de casas inteligentes pode impactar no sucesso ou fracasso de um projeto, com base em um plano de gerenciamento de risco de qualidade e muito bem mapeado, devem-se elaborar respostas aos prováveis riscos identificados na fase de Iniciação do Projeto.

Conforme vimos no decorrer do artigo existem diversas maneiras de identificar e mapear as vulnerabilidades da rede que poderão se tornar risco, através de algumas técnicas é possível identificar e posteriormente planejar ações que venham a minimizar os riscos.

Durante a elaboração deste artigo focamos em 3 tópicos que julgamos de grande importância para a segurança em projetos de Casas Inteligentes, *softwares*, dispositivos ou sensores e *Firmwares*.

Pode-se afirmar que ao identificar um risco com maior antecedência, tornará mais fácil sua tratativa e assim posteriormente diminuirá sua exposição a ataques.

Seguem alguns aspectos que foram abordados no decorrer deste artigo:

- Boas práticas de projeto;
- Confidencialidade dos Dados, Autenticação e Controle de Acesso;
- Capacidade de Atualização;
- Regulamentação;
- Padrões e métricas;
- Disponibilidade;
- Obsolescência de dispositivos;

Os itens citados acima quando tratados com a devida atenção, tendem a minimizar o risco. Praticamente todos os aspectos citados possuem uma correlação entre si, as Boas Práticas em Projetos, funciona como um integrador englobando os demais aspectos.

**Custo versus Segurança** está relacionado diretamente com a sua **capacidade de atualização** e seu tempo de **Obsolescência**. Pois, os dispositivos mais baratos provavelmente terão menor capacidade de atualização e consequentemente um ciclo de vida menor, tornando-o obsoleto em menos tempo do que se espera.

Com relação a falta de regulamentação no setor, isto pode impactar na confidencialidade dos dados e nos controles de acesso aos dispositivos.

Portanto, pode-se concluir que para minimizar os riscos em projetos de Casas Inteligentes não existe uma formula única para tal, trata-se de um conglomerado de ações e decisões mais abrangentes, que devem ser tomada com um determinado embasamento técnico, esse conjunto de ações se inicia desde o começo do projeto, através da escolha das melhores práticas a serem executadas no projeto, definições de padrões de desenvolvimento e métricas de codificação, passando pelas escolhas e compras de dispositivos de alta qualidade e baixa vulnerabilidade até o fim da execução do projeto, que podemos exemplificar com o serviço *Cloud Computing* a ser escolhido para armazenar esses dados que serão trafegado. Ou seja, o conjunto de ações corretas tornará o projeto mais seguro e menos vulnerável.

## REFERÊNCIAS

ABRAHAM, E. **Gestão de Risco em Projetos: Uma análise do projeto COR da Infoglobo**. Trabalho de Conclusão de Curso (Graduação em Administração de Empresas). Orientado pela professora Ms. Claudia Rosana Felisberto Scofano. Centro Universitário Metodista Bennett, Rio de Janeiro, 2012.

BARALDI, P. **Gerenciamento de Riscos**. 3. ed. Rio de Janeiro: Campus, 2010.

BART BROECKMAN, B.; NOTEMBOOM, E. **Testing Embedded Software**. Chicago: Addison Wesley Professional, 2002.

COOPER, D.; GREY, S.; RAYMOND, G.; WALKER, P. **Project Risk Management Guidelines:** managing risk in large projects and complex procurements. England: John Wiley & Sons, 2005. 384 p. Disponível em: <http://library.aceondo.net/ebooks/Business_Management/Project.Risk.Management.Guidelines..pdf>. Acesso em: 26 de outubro de 2018.

JACOBSSON, A.; BOLDT, M.; CARLSSON, B. 2016. **A risk analysis of a smart home automation system**. Future generationcomputer system, v. 56, p. 719–733. Disponível em: <https://www.semanticscholar.org/paper/A-risk-analysis-of-a-smart-home-automation-system-Jacobsson-Boldt>. Acesso em: 14 de outubro de 2018.

KERZNER, H. **Gerenciamento de projetos:** uma abordagem sistêmica para planejamento programação e controle. 10. ed. São Paulo: Blucher, 2011.

KENDRICK, T. **Identifying and managing project risk**: essential tools for failure-proofing your project. New York: Amacom, 2003.

LINHARES, J.; QUARTAROLI, C. M. **Guia do gerenciamento de projetos e certificação PMP**. 1. ed. Rio de Janeiro: Ciência Moderna, 2004.

NASCIMENTO, V. M. **Gerência de riscos em planejamento e controle de projetos**. Monografia Graduação em Administração de Empresas pela Universidade Veiga de Almeida – UVA, Orientador: Aluisio Monteiro, M.Sc. Rio de Janeiro. 2003. Disponível em: <https://www.uva.br/sites/all/themes/uva/files/pdf/monografia-gerenciamento-de-risco-em-projetos.pdf>. Acesso em: 18 de outubro de 2018.

NEVES, S. M.; SILVA, C. E. S. **Gestão de riscos aplicada a projetos de desenvolvimento de software em empresas de base tecnológica incubadas**: revisão, classificação e análise da literatura. Gest. Prod. São Carlos, v. 23, n. 4, p. 798-814, dez. 2016. Disponível em: <http://dx.doi.org/10.1590/0104-530x472-15>. Acesso em: 24 de setembro de 2018.

PALMA, M. A. M.; ANDRADE, J. L. P.; SILVA, J. **Revista de Gestão de Projetos**: Gestão de riscos em projetos: Contornando incertezas para viabilizar a implantação de nova tecnologia em uma indústria petrolífera de E&P. Ensaio: avaliação e políticas públicas em educação, São Paulo, v. 2, n. 2, p. 102-122, jul./dez. 2011. Disponível em: <https://www.thefreelibrary.com/_/print/PrintArticle.aspx?i

d=281461843>. Acesso em: 22 de setembro de 2018.

PROJECT MANAGEMENT INSTITUTE. **Guia PMBOK®: Um Guia para o Conjunto de Conhecimentos em Gerenciamento de Projetos.** 4. ed., Pennsylvania: PMI, 2008. Disponível em: <https://tarciocaldas.files.wordpress.com/2010/04/pmbok-4c2aa-edicao.pdf>. Acesso em: 25 de setembro de 2018.

SCOFANO, C. R. F.; ABRAHAM, E. F.; SILVA, L. S.; TEIXEIRA, M. A. **Gestão De Risco Em Projetos: Análise das etapas do PMI-PMBOK (Project Management Institute)**. In: XI Congresso Online de Administração, 2013, Brasília. **Anais** do XI Congresso Online de Administração, 2013. Disponível em: <http://www.convibra.org/upload/paper/2013/36/2013_36_8214.pdf>. Acesso em: 20 de setembro de 2018.

SILVA, F. L. A. **Análise do impacto do gerenciamento de riscos no sucesso de projetos**: um estudo de caso em uma organização de desenvolvimento de software. Dissertação (Mestrado Ciência da Computação). Centro de Informática da Universidade Federal de Pernambuco. Recife, PB. fev. 2013. 112 f. Disponível em:<https://repositorio.ufpe.br/handle/123456789/19689>. Acesso em: 10 de outubro de 2018.

STEFFEN JUNIOR, J. **Gerenciamento de risco em TI**: um estudo de caso voltado a falhas e incidentes. 2011. 51 p. Monografia Pós-Graduação Gestão de Negócios Financeiros. Escola de Administração, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2011. Disponível em: <http://www.lume.ufrgs.br/handle/10183/77527>. Acesso em: 24 de outubro de 2018.

WALLACE, L.; KEIL, M. 2004. **Software project risks and their effect on outcomes**. Communications ofthe ACM, v. 47, n. 4, p. 68–73. Disponível em: <https://dl.acm.org/citation.cfm?doid=975817.975819>. Acesso em: 20 de outubro de 2018.

WILSON, C.; HARGREAVES, T.; HAUXWELL BALDWIN, R. 2017. **Benefits and risk os smart home technologies**. Energy Policy, v. 103, p. 72–83. Disponível em: <https://www.sciencedirect.com/science/article/pii/S030142151630711X>. Acesso em: 16 de outubro de 2018.