
# "Cyber Security: a pillar for smart cities"

Mestrado em Cibersegurança e Informática Forense

Paulo José Santos Vaz

Leiria, setembro de 2019


# “Cyber Security: a pillar for smart cities”

Mestrado em Cibersegurança e Informática Forense

Paulo José Santos Vaz

Trabalho de Projeto realizado sob a orientação do Professor Doutor Luís Alexandre Lopes Frazão e do Professor Doutor Jorge Manuel Ferreira Barbosa Ribeiro do Instituto Politécnico de Viana do Castelo

Leiria, setembro de 2019

# Originalidade e Direitos de Autor

O presente relatório de projeto é original, elaborado unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para a/o elaborar.

# Agradecimentos

Gostaria de agradecer a todos que de forma direta ou indireta contribuíram para o sucesso da conclusão desta etapa da minha vida.

Em primeiro lugar, gostaria de agradecer ao meu orientador, Professor Doutor Luís Frazão, por toda a disponibilidade, apoio e por toda a atenção concebida.

Ao meu coorientador, Professor Doutor Jorge Ribeiro do Instituto Politécnico de Viana do Castelo pela disponibilidade, e o apoio incansável prestado ao longo desta dissertação.

À Joana pela motivação e por sempre acreditar em mim.

Ao Miguel que me deu a dica que me fez iniciar na temática da Cibersegurança, "*Até já ma man".*

À minha família por todo o suporte e ausências.

# Resumo

O conceito de Cidades Inteligentes ou "Smart Cities" (SC) é definido de forma diversa na literatura mas em suma pode ser descrito como um conceito que se refere a uma integração, baseada em tecnologia, dos aspetos sociais e económicos de uma cidade, com o objetivo de potenciar o desenvolvimento sustentável e resiliente de uma cidade melhorando a qualidade de vida dos cidadãos. Tendo em consideração o desenvolvimento tecnológico e o aumento de um grande número de serviços e processos associados às SC, que assentam em infraestruturas tecnológicas, Sistemas e Tecnologias de Informação (SI/TI) e redes digitais, estes devem ser protegidas e geridas de forma a apoiar o controlo dos processos de prestação desses serviços.

Nas últimas décadas, várias orientações para a gestão e controlo dos SI/TI, como ISO 27001, COBIT e ITIL, foram apresentadas. Por outro lado, a cibersegurança é uma das tendências e preocupações mais recentes em relação à segurança de TI e, em particular, em termos de suporte à infraestrutura tecnológica das SC.

Seguindo uma metodologia investigação-ação para responder à pergunta "A cibersegurança é um pilar necessário das Smart Cities?", foi aplicada a uma SC uma lista de verificação do estado da Cibersegurança, assim como identificadas um conjunto de linhas orientadoras baseadas em referências internacionais e mundiais para mitigar os riscos das vulnerabilidades associadas à cibersegurança.

Podemos concluir que é possível responder à questão de forma positiva e considerar a existência do relacionamento entre as SCs e a cibersegurança, assim como delinear um conjunto de questionários e orientações muito especificas para mitigar as vulnerabilidades associadas à infraestrutura tecnológica de suporte aos serviços disponibilizados pelas SC.

**Palavras-chave:** Cibersegurança, Cidades Inteligentes, Tecnologias de Informação

# Abstract

Smart City (SC) is a concept that is differently defined in the literature and can be described as a concept that refers to a technology-based integration of both social and economic aspects of a city in order to sustain sustainable and resilient development. Due to technological development, a large number of smart city services and processes are based on technological infrastructures, information systems and digital networks, which must be secured and managed in such a way as to support the control of the SC processes. Various guidelines for the management and control of IT such as ISO 27001, COBIT and ITIL have been presented. On the other hand, Cybersecurity is one of the most recent trends and concerns regarding IT security in general and, in particular, in terms of Intelligent Infrastructure. Following a method of action to answer the question Is Cybersecurity a necessary pillar of SCs? it was applied a series of cybersecurity checklists to a real case of a middle city board with a defined SC structure. It may be over and done with that it is possible to achieve the objectives that should be associated with the relationship between SCs and Cybersecurity, and to obtain specific and important information in the specification of a learning method in order to achieve the proposed intentions and to defuse the planned question.

**Keywords:** Cybersecurity, Smart Cities, Information Technology

# Índice

# Lista de Figuras

# Lista de tabelas

# Lista de siglas, acrónimos e notação

| | |
|---|---|
| AR | Action Research |
| COBIT | Control Objectives for Information and Related Technology |
| DSR | Design Science Research |
| EUA | Estados Unidos da América |
| IoT | Internet das Coisas ou ”Internet of Things” |
| NIST | Cyber Security Systems Framework |
| OWASP | Open Cyber Security Framework |
| SC | Smart City ou Cidade Inteligente |
| SANS | SANS Critical Security Controls for Effective Cyber Defense |
| SI | Sistemas de Informação |
| SI/TI | Sistemas de Informação/Tecnologias de Informação |
| TI | Tecnologias de Informação |
| TIC | Tecnologia de Informação e Comunicação |

A secção das Referências está estruturada em duas subsecções: uma referente à bibliografia e outra referente às referências bibliográficas. No sentido de facilitar a leitura e a indicação de referências, neste trabalho sempre que nos referenciamos a um trabalho científico seguimos a indicação do apelido dos autores, encontrando-se a lista na seção “bibliografia”. Exemplo “..(Khatoun e Zeadally, 2017),..”

> Khatoun, R. e Zeadally, S. (2017). *Cybersecurity and Privacy Solutions in Smart Cities*. IEEE Communications Magazine IEEE Commun. Mag. Communications Magazine, IEEE. 55(3):51-59.

Sempre que nos referimos a relatórios ou informação da literatura digital, seguimos a indicação de números, estando listada na secção “referências bibliográficas”. Exemplo “…[1]…”:

> [1] Josep-Ramon Ferrer (2017). *Barcelona’s Smart City vision: an opportunity for transformation. Journal of Field Actions Science Reports*. Special Issue 16, p.70-75. Disponível em: https://journals.openedition.org/factsreports/4367

# 1. Introdução

A terminologia das cidades inteligentes ou "Smart Cities" (SC), corresponde a um conceito que, embora convirjam no mesmo sentido, pode ser definido de maneira diferente na literatura escrita e online. Em termos gerais, as SC centram-se na disponibilização de um conjunto de iniciativas, ações, serviços, em várias áreas de aplicabilidade das cidades (com ou sem tecnologia associada) que visam otimizar e melhorar o bem estar das populações, quer em termos de saúde quer em termos de ambiente. Na realidade existe uma grande variedade de áreas em que as cidades se podem tornar mais "inteligentes". Vários autores/investigadores apresentam algumas definições, como de Lévy-Bencheton e Darra (2015) que referem que as SC são uma evolução das "cidades conectadas" com a prevalência na transferência de dados em grande escala. Embora seja possível reunir diferentes definições do conceito de SC, destacando o caráter não unificado do conceito, poderemos considerar que de alguma forma, é consensual que o conceito de SC tenha nascido para proporcionar uma melhor qualidade de vida aos cidadãos. Neste sentido, em termos gerais, o objetivo das SC centra-se em otimizar a cidade de forma dinâmica, a fim de disponibilizar um conjunto de ações e serviços perspetivando uma melhor qualidade de vida aos cidadãos (Khatoun e Zeadally, 2017) podendo, em certa medida, ser melhorada a sua eficiência e eficácia através da aplicação das Tecnologia de Informação e Comunicação (TIC). A principal ideia em utilizar as TIC nas SC é a de integrar serviços de Sistemas de Informação (SI) de cada domínio de atividade de uma cidade, como as áreas da saúde, educação, transporte, energia, gestão de água e resíduos, de modo a disponibilizar serviços públicos aos cidadãos de uma maneira mais eficiente e omnipresente (Bawany e Shamsi, 2015) tipicamente operando num ambiente urbano dinâmico, incorporando vários sistemas complexos quer a nível de serviços e a nível da infraestrutura tecnológica (Zhiyi e Shahidehpour, 2017) (Hazel e Taeihagh, 2018), quer a nível do comportamento humano, tecnologia, estruturas sociais, políticas, assim como na economia envolvente associada às cidades (Gaur et al. 2015), (Zhen e Qi 2018).

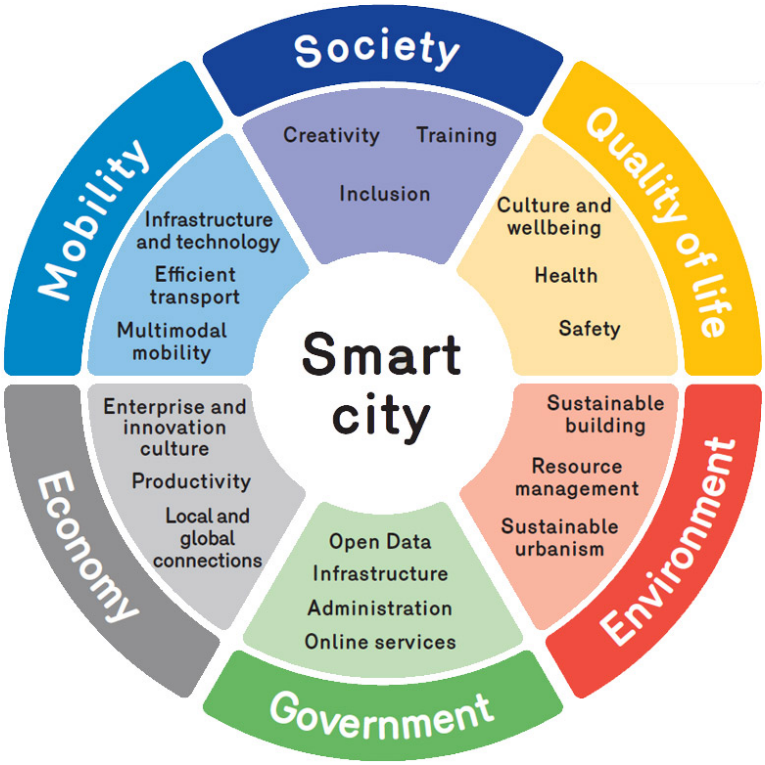


**Figura 1.1 – Esquemático geral dos domínios associados às Cidades Inteligentes (Fonte: *Brussels Smart City*).**

Na figura 1.1 (*Fonte: Brussels Smart City*[1]) são ilustrados os domínios gerais associados às SC. Embora possam ser esquematizados de uma forma mais ou menos abrangente, os principais domínios correspondem aos da sociedade, qualidade de vida, ambiente, governança, economia e mobilidade, podendo ser acrescidos de outros associados, como saúde, construção, tecnologia e infraestrutura, entre outros. Partindo destes domínios (e como exemplo o ilustrado na figura 1.1), estes podem ser subdivididos em outros domínios mais específicos, como por exemplo, para o domínio da qualidade de vida, ser subdividido em cultura e bem-estar, saúde e segurança.

Por outro lado, é amplamente conhecido e consensual referir que as TIC aplicadas nas SC disponibilizam um vasto conjunto de oportunidades para as pessoas/cidadãos criarem, inventarem, testarem e experimentarem "coisas novas", de modo a melhorar e otimizar na sua qualidade de vida ou na de terceiros. Contudo, tendo em consideração a exposição dos serviços digitais e serviços de suporte dos vários domínios através de redes de comunicação e de utilização de TI e SI, é importante ter em consideração a identificação de riscos e

[1] https://smartcity.brussels/the-project-definition

desafios associados às SC quando assentes em SI/TI, de modo a reduzir ou mitigar esses riscos, nomeadamente em diferentes setores de atividade, como por exemplo nos sistemas de controlo industrial, sistemas inteligentes de transporte, Internet das Coisas (IoT), saúde digital (*e-health*), além de outras áreas de intervenção das cidades.

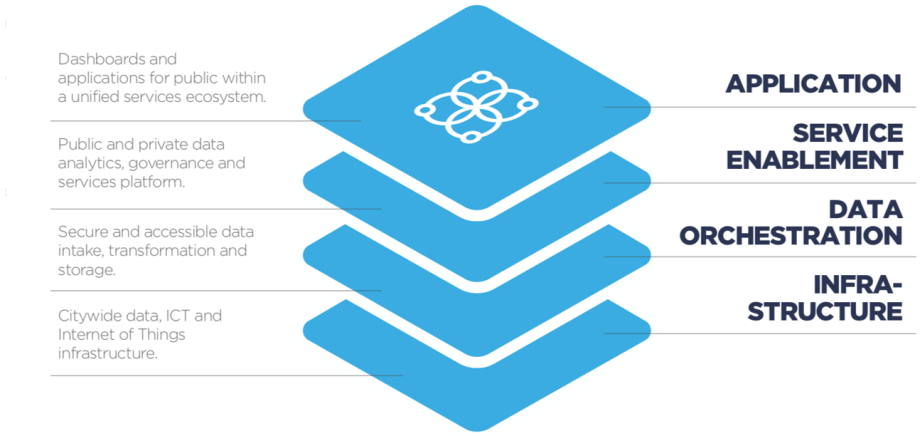


**Figura 1.2 – Arquitetura geral da camada de aplicação das TIC no contexto das Cidades Inteligentes (Bin Bishr, 2015).**

Na figura 1.2 (Bin Bishr, 2015) é ilustrado um exemplo de uma arquitetura geral da camada de aplicação das TIC no contexto das SC. Nesta ilustração, evidencia-se a hierarquia baseada na infraestrutura tecnológica onde assentam transferência de dados (*data orchestration*), a disponibilização de serviços digitais (*servisse enablement*), assim como a camada aplicacional (*application*) que disponibiliza aos cidadãos as interfaces de utilização dos serviços digitais.

Contudo, tendo em consideração a evolução da sociedade e dos SI/TI, a segurança informática e as questões associadas à privacidade dos dados tornaram-se cada vez mais pertinentes, questionáveis e desafiadoras, quer para os cidadãos, quer para as empresas tecnológicas que disponibilizam serviços digitais atentos à problemática do cibercrime e do ciberterrorismo. Neste sentido, surge o conceito da "cibersegurança", que tem como objetivo centrar-se na segurança dos dados, das aplicações informáticas e da infraestrutura tecnológica que é usada para armazenar, processar e transferir esses mesmos dados aos cidadãos, entre serviços digitais, aplicações informáticas, equipamentos IoT, etc.

Neste contexto, e no âmbito do plano curricular do mestrado e considerando que uma dissertação de mestrado tem por objetivo a realização de um trabalho de investigação que conduza à preparação de uma dissertação de natureza científica sobre um tema da área de

conhecimento do curso e enquanto que um o trabalho de projeto tem como objetivo a aplicação integrada de conhecimentos e de competências adquiridos ao longo do curso a situações novas de interesse prático, através da adoção de metodologias e estratégias apropriadas com vista à resolução ou exploração de uma solução ou resposta a questões de investigação associados a um problema específico das áreas de conhecimento do curso, consideramos que a aplicabilidade deste trabalho corresponde a um trabalho de projeto de mestrado, o qual se baseia nas temáticas das SC e da cibersegurança e o qual se centra em responder à seguinte questão de investigação: "A cibersegurança é um pilar das Smart Cities?". Para responder a esta questão nas próximas secções apresentamos a motivação, os objetivos e a metodologia de investigação utilizada, sendo que nas secções dois e três apresentamos a parte principal do estudo e de aplicabilidade a um caso de estudo (a uma SC).

## 1.1. Motivação

O presente trabalho de projeto de mestrado procura apresentar estudar, identificar e aplicar um conjunto de orientações a um caso de estudo, uma SC, de modo a puder responder de forma positiva à questão se a cibersegurança é um pilar para as cidades inteligentes ou SC. Dado o crescimento da terminologia SC e do crescimento real e efetivo das tradicionais cidades para "cidades inteligentes" e, tendo em consideração, por um lado, que grande parte do domínio característicos das SC disponibilizam serviços digitais em que os dados e informação são disponibilizados e transferidos sobre diferentes plataformas SI/TI e que a cibersegurança, aliada à segurança informática, se torna cada vez mais relevante em reduzir e mitigar os riscos inerentes aos ciber ataques e ciberterrorismo, a motivação deste trabalho centra-se na identificação das melhores normas, orientações, *frameworks*, não só orientadas para a segurança informática, mas em particular para a cibersegurança quando associada aos serviços disponibilizados pela infraestrutura tecnológica das SC quando estas utilizam os SI/TI.

## 1.2. Objetivos

Neste contexto, utilizando uma metodologia de investigação ação (descrita na secção seguinte), o principal objetivo deste trabalho é responder à questão "É a cibersegurança um pilar necessário das Smartcities?". Para a concretização do objetivo global foram definidos os seguintes sub-objetivos:

- Revisão da Literatura e estudo do estado da arte associado às SC, segurança informática e cibersegurança;
- Identificação e estudo de um conjunto de linhas orientadoras, normas e *frameworks* utilizadas a nível mundial para avaliar e mitigar a problemática associada à segurança informática e à cibersegurança em especial, quando aplicados às SC.
- Definição de uma lista de verificação (*checklist)* do estado da relação SC com a cibersegurança em cenários em que as SC assentam os seus serviços em SI/TI;
- Aplicação da lista de verificação a um caso de estudo real;
- Análise, discussão de resultados e divulgação das conclusões.

Para concretizar estes objetivos definiu-se uma estratégia (ou orientação) materializada através de um conjunto de etapas. Sendo a base do trabalho os conceitos, particularidades e características a ter em consideração nas SC e na cibersegurança, após o estudo e análise da literatura escrita, online e em eventos tecnológicos, centrados numa fase inicial num caso de estudo de uma SC, iniciamos o trabalho com o mapeamento entre os domínios da SC e a abrangência e aplicabilidade das normas, *standards* e *frameworks* da cibersegurança (e segurança informática) mais conhecidos e utilizados a nível mundial. Com base neste mapeamento, e para cada relação de domínio das SC, com a estrutura hierárquica de itens das normas, standards e *frameworks* identificou-se um conjunto de questões de análise, a fim de construir uma lista de verificação do estado da relação das SC face à cibersegurança, no sentido de quantificar e avaliar a exposição da infraestrutura tecnológica das SC a situações de cibersegurança.

Com esta lista de verificação, assim como um conjunto de orientações práticas associadas aos vários itens de análise da cibersegurança face à infraestrutura tecnológica de suporte às SC, aplicamos a um caso de estudo. Como resultado direto deste trabalho pretendeu-se:

- Criar uma lista de verificação o mais abrangente possível sobre cibersegurança passível de ser testada numa infraestrutura tecnológica de uma SC para avaliar o seu estado de situação em relação à cibersegurança;
- Apresentar um conjunto de linhas orientadoras associadas à segurança informática e à cibersegurança em particular passíveis de complementar a informação a ser analisada em cada item de análise na infraestrutura tecnológica das SC.

Como resultado indireto deste trabalho, mas enriquecedor em termos de conhecimento adquirido, o estudo das características, particularidades, problemáticas, casos de estudo reais, linhas orientadoras, normas e *frameworks* associados às SC e à cibersegurança em particular na literatura escrita, online e em eventos tecnológicos mundiais, assim como na aplicabilidade de uma lista de verificação do estado da Cibersegurança numa SC, servirá para aumentar os conhecimentos sobre estas temáticas e efetuar um primeiro teste de aplicabilidade real na análise do estado da cibersegurança numa SC.

## 1.3. Metodologia de Investigação e Plano de Trabalho

Vário estudo tem sido apresentados e utilizados como métodos de pesquisa (Kilani e Kobziev, 2016) aplicados a casos de estudo na investigação e desenvolvimento, como as metodologias Action Research (AS) (Aviso net al. 1999) (Olesen e Myers, 1999) ou Design Science Research (DSR) (Hevner et al. 2004) (Peffers et al. 2007). A DSR é bastante utilizada no desenvolvimento de soluções de software ou em projetos de SI/TI, sendo estruturada num conjunto de etapas e ciclos como a identificação e motivação para o problema em análise; definição dos objetivos da solução para o problema; desenho e desenvolvimento da solução e por fim demonstração, avaliação e comunicação. Por outro lado, a metodologia DSR poderá ser combinada com a AR para investigar os requisitos e a investigação, assim como a implementação e avaliação do projeto. Neste trabalho foi usada a metodologia AR para a "resolução de um problema" a qual foi aplicada a um caso de estudo em que é expectável se responder a uma questão de investigação. Usando este método, o investigador testa em ambiente real, obtém o feedback, modifica a "teoria" e segue em "frente" na concretização dos objetivos. De acordo com Olesen e Myers (1999) são usadas cinco etapas no método AR que incluem:

- Diagnóstico (*Diagnosing*) - identificar a questão de investigação. Neste trabalho a questão de investigação é seguinte "É a cibersegurança um pilar das smartcities?";
- Planeamento da Ação (*Action Planning*) - Determinar as ações a serem tomadas para conseguir responder à questão de investigação;
- Tomada da Ação (*Action Taking*) - Conduzir e monitorizar as ações planeadas;
- Avaliação (*Evaluation*) – Determinar se as ações foram adequadas para conseguir responder à questão de investigação e,
- Aprendizagem Obtida (*Specifying Learning*) – A aprendizagem obtida com todo o processo da investigação.

Assim, de modo a atingir os objetivos definidos e responder à questão de investigação usando a metodologia AR as ações foram divididas em várias etapas (ou fases) (Figura 1.4):

- Fase A – Revisão da Literatura: Nesta fase, foi recolhida o máximo de informação da literatura escrita e online de modo a estudar e perceber todos os conceitos, problemáticas e particularidades atuais, quer das SC, quer da cibersegurança (e da segurança informática).
- Fase B – Estado da Arte - Nesta fase foram registados os trabalhos de investigação mais relevantes e recentes sobre as temáticas envolvidas, a análise das temáticas de eventos tecnológicos de nível mundial, a análise e estudo das normas, orientações, *frameworks* e casos de estudo de aplicabilidade da cibersegurança em particular em SC assentes em infraestruturas tecnológicas de suporte aos serviços disponibilizados aos cidadãos.
- Fase C – Desenvolvimento de uma lista de verificação do estado da cibersegurança no que se refere ao estado de situação da cibersegurança nas SC, assim como indicar um conjunto "boas práticas/orientações" mundialmente conhecidas passíveis de serem testadas em SC para mitigar a problemática da cibersegurança.
- Fase D – Teste real da lista de verificação do estado da cibersegurança, relação da cibersegurança aplicada a SC). No final desta fase serão analisadas as conclusões e a aprendizagem obtida, assim como delinear passos futuros para melhorar o desempenho da investigação.
- Fase E – Escrita do relatório de projeto e divulgação – Redação do documento do projeto e proceder à divulgação dos resultados do trabalho, principalmente em conferências e em seminários/palestras do conselho onde se insere a SC de estudo.

O plano de tese é apresentado na Figura 1.4

| Fases | | 2018 | | 2019 | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Nov | Dez | Jan | Fev | Mar | Abr | Mai | Jun |
| A | Revisão da Literatura | X | X | | | | | | |
| B | Estado da Arte | | X | X | | | | | |
| C | Desenvolvimento da lista de verificação | | | X | X | X | | | |
| D | Teste e Avaliação | | | | | X | X | X | |
| E | Escrita do relatório do projeto e divulgação | | | X | | X | X | X | X |

**Figura 1.3 - Escalonamento do plano de trabalhos.**

## 1.4. Estrutura do Documento

O presente documento encontra-se dividido em seis capítulos. No primeiro capítulo é apresentada a introdução, uma breve contextualização e um enquadramento, motivação e os objetivos, assim como a metodologia de investigação seguida.

No Capítulo 2 é apresentado o estado da arte referente aos conceitos de SC, segurança e cibersegurança, um breve estudo sobre as temáticas abordadas em eventos tecnológicos mais recentes, assim como as principais normas, *guidelines* e *frameworks* passíveis de serem aplicadas às SC no âmbito da Segurança e cibersegurança. Ainda neste capítulo é apresentada uma *checklist* global que consideramos passível de ser aplicada às SC, a qual foi testada num caso de estudo apresentado no capítulo seguinte.

No Capítulo 3 apresenta-se um caso de estudo de uma SC e no capítulo 4 as conclusões e trabalho futuro. No final apresentam-se a bibliografia e as referências bibliográficas que sustentaram a componente científica e de investigação teórica e prática deste trabalho. Para terminar apresenta-se no anexo o artigo publicado numa conferência internacional com indexação SCOPUS. Com base nestes conhecimentos e nesta lista de verificação no capitulo três apresentamos o caso de estudo alvo do projeto e no quarto as conclusões e trabalho futuro.

# 2. Estado da Arte

Neste capítulo pretende-se apresentar o "estado da arte" sobre Smart Cities, segurança informática e cibersegurança. Iniciamos com a análise do estudo da literatura escrita e online mais recentes associadas à aplicabilidade das SC, segurança informática e cibersegurança, assim como um resumo das temáticas mais relevantes de um conjunto de eventos tecnológicos mundiais associados às SC e em particular à cibersegurança. Desta forma, pretendeu-se recolher o máximo de informação e conhecimento para o desenvolvimento deste trabalho. De seguida, apresentamos um conjunto de exemplos de casos reais de aplicabilidade da cibersegurança a SC. Depois apresentamos as principais orientações, normas e *frameworks* que se focam na cibersegurança (e na segurança informática), apresentamos uma proposta de lista de verificação (*checklist*) passível de ser aplicada numa SC para analisar o estado da sua cibersegurança, ou, por outras palavras, o estado de situação da cibersegurança da sua infraestrutura tecnológica quando os serviços da SC assentam em SI/TI. A variedade de áreas onde as cidades se podem tornar "inteligentes" é extensiva, podendo ser considerada por vários autores como uma evolução das cidades conectadas com predominância na transferência de informação em grande escala (Lévy-Bencheton e Darra, 2015). No entanto, é possível reconhecer um ponto comum nas diferentes definições do conceito de SC: as SC têm como objetivo melhorar a qualidade de vida dos cidadãos. Vários autores apresentam várias definições, mas todos convergem para este objetivo, como os seguintes trabalhos (Monzon, 2015) (Bawany e Shamsi, 2015) (Gaur et al, 2015) (Ayoub et al, 2016) (Ijaz et al. 2016) (Mijac et al. 2017) que evidenciam e salientam a importância do dinamismo na otimização dos serviços das SC para disponibilizar aos cidadãos uma melhor qualidade de serviço e de vida potenciando o uso dos SI/TI.

Neste sentido, e tendo em consideração a evolução tecnológica, evidencia-se o aumento em grande escala de serviços que potenciam a utilização dos SI/TI através da integração ou interoperabilidade de SI/TI em vários setores (como a saúde, educação, transportes, energia, recursos hídricos e gestão de desperdícios) de modo a disponibilizar aos cidadãos formas mais eficientes (Monzon, 2015) (Bawany e Shamsi, 2015), "amigas" do ambiente e que envolvam um ambiente urbano dinâmico e complexo assente em SI/TI numa (ou várias) infraestruturas tecnológicas (Mijac et al. 2017) (Armin et al. 2017) (Lim e Taeihagh 2018), assim como o dinamismo associado às dimensões do comportamento humano, social,

politico e económico das cidades (Evans et al. 2016) (Li e Liao 2018). Por outro lado, a aproximação das SC aos cidadãos origina o aparecimento de novos desafios como por exemplo o de promover o acesso à informação disponibilizada e utilizada pelos cidadãos não descurando asas questões implícitas de confidencialidade e integridade. No atual conceito de SC o tratamento de fatores individuais deve permitir desenvolver serviços de uma forma global, multi-fatores/muti dimensões (sociais, económicas, políticas, etc.) [1]. Esta particularidade é ainda mais relevante quando duas dimensões emergem ou evidenciam-se, nomeadamente da "governança inteligente" ("smart governance") e as "pessoas inteligentes" ("smart people").

Todos estes aspetos competem com o atual conceito de SC para se desenvolver em várias áreas de atuação, ou pilares estratégicos, tendo sido já apresentados e difundidos a nível mundial como casos de estudo e de sucesso, como por exemplo os estudos, (Angelidou, 2016) (Khan et al. 2017) (Jansäter e Olsson, 2018), os planos estratégicos nas cidades do Dubai [2, 3], Londres [4], cidade de Barcelona [5], cidade de London (Canadá) [6], Viena de Áustria [7], cidade de NewCastle [8], cidade de Edmonton [9], cidade de St. Albert – Estados Unidos da América (EUA) [10], assim como relatórios associados à análise da cibersegurança em vários países e relatórios de empresas consultoras de renome mundial [11-14]. Na figura 2.1 (obtida em www.smartcitiesworld.net) ilustra a grande variedade de dimensões e categorias quando se associa as SC aos SI/TI.


**Figura 2.1 – Ilustração dos vários domínios associados às Smart Cities (www.smartcitiesworld.net)**

Neste contexto, poderemos considerar as seguintes categorias (ou domínios) que englobam as SC:

- Energia inteligente (*Smart Energy* – Gestão digital de energia, *Smart Grids*, Medidores inteligentes (*Smart Meters*) e armazenamento inteligente de energia;
- Edifícios Inteligentes (*Smart Buildings*) – Automação eficiente de edifícios, Sistemas avançados de refrigeração e ventilação do ar, equipamentos inteligentes de iluminação;
- Mobilidade Inteligente (*Smart Mobility*) – Mobilidade inteligente, sistemas avançados de gestão de tráfego, gestão inteligente de parques, sistemas inteligentes de transporte;
- Tecnologia Inteligente (*Smart Technology*) – Sistemas avançados de conetividade, 4G e 5G, largura de banda em grande escala, redes sem fios gratuitas;
- Infraestrutura Inteligente (*Smart Infraestructure*) – Gestão digital da infraestrutura, redes de sensores, sistemas digitais de gestão e controlo de recursos hídricos, gestão de desperdícios;
- Governança Inteligente (*Smart Governance*) e Educação Inteligente (*Smart Eucation*) – Plataformas digitais de disponibilização de serviços públicos, *e-Government*, serviços digitais para a educação (*e-Education*), soluções de gestão de desastres;
- Saúde Inteligente (*Smart Healthcare*) – Tecnologias inteligentes para a saúde, disponibilização de serviços digitais na saúde através de vários dispositivos móveis (*e-Health* e *m-Health*), Sistemas inteligentes de ligação entre equipamentos médicos.
- Cidadãos Inteligentes (*Smart Citizen*) – Uso de opções de mobilidade verde, diferentes opções de melhoramento da qualidade de vida, acesso a conteúdos e serviços digitais;
- Segurança Inteligente (*Smart Security*) – Deteção inteligente de ameaças, sistemas biométricos, modelos de simulação e de previsão de proteção de crimes, sistemas avançados e proativos de proteção (anti-virus).

Neste sentido, as aplicações finais de cada um destes domínios correspondem a um conjunto de objetivos a atingir que podem estar diretas ou indiretamente interligados com outros domínios da caracterização das SC, devendo ser simples a implementação de uma infraestrutura global em que os recursos físicos e tecnológicos possam recolher, armazenar,

processar e disponibilizar um conjunto de serviços aos cidadãos para cada um dos domínios *Smart.*

Contudo, tendo em consideração a larga abrangência de domínios e envolvência de vários SI/TI, torna-se necessário avaliar a maturidade de uma SC. Para isso podemos destacar a nível europeu, as ferramentas de avaliação *European Smart Cities Maturity Assessment* [15] (Figura 2.2) e a *European SCs Benchmarking Assessment* [16] (Figura 2.3).]. Neste tipo de ferramentas, a avaliação é baseada em pesos nas várias dimensões associadas às SC, obtida a informação através de questionários ou inquéritos.

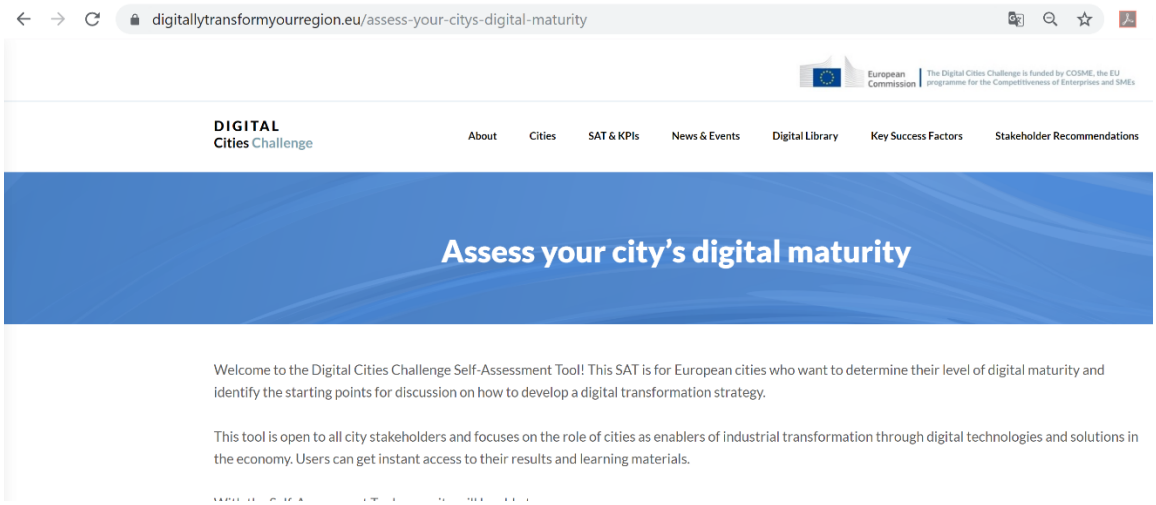


**Figura 2.2 – Ilustração da ferramenta European Smart Cities Maturity Assessment [15].**

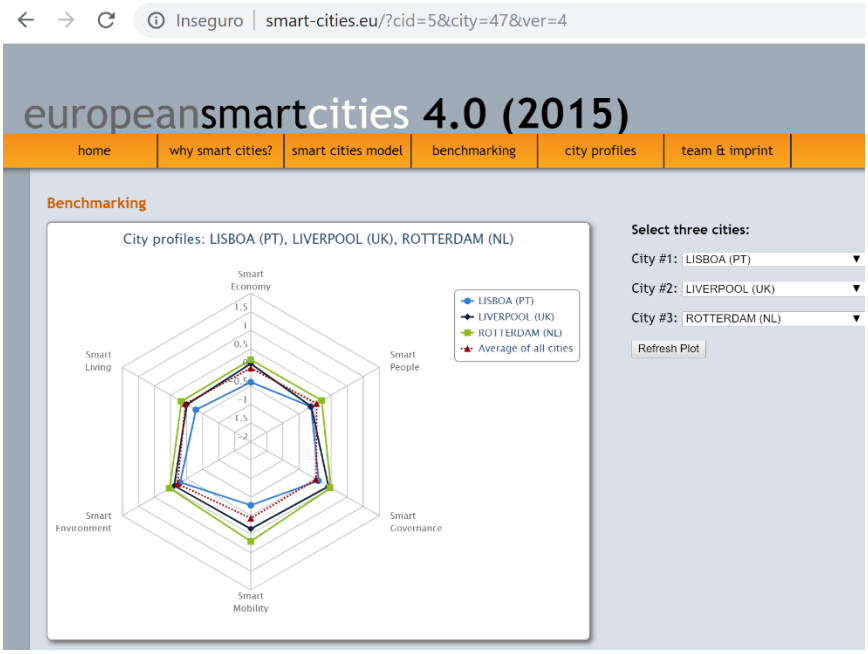


**Figura 2.3 – Ilustração da ferramenta European Smart Cities Benchmarking Assessment [16].**

Associando-se ao desenvolvimento das SC, a segurança e privacidade dos dados tem vindo a ser uma preocupação para os cidadãos, entidades governamentais e para as empresas, que tem vindo a apresentar vários desafios na redução ou mitigação dos riscos associados à cibersegurança. A cibersegurança trata da segurança dos dados e das aplicações e da infraestrutura usados para armazenar, processar e transmitir/transferir dados. Entende-se como o processo de proteção de dados e informações, a prevenção, a deteção e a resposta a eventos de cibersegurança. Tais eventos, incluindo ataques intencionais e acidentes, correspondem a mudanças que podem afetar as operações das instituições (e empresas) (Ijaz et al., 2016) (Zhang et al, 2017). Muitas outras leis (ou formas legais) necessitam de ser padronizadas e publicadas de modo a permitir de forma mais confiável e segura a conetividade de serviços e de equipamentos (ex. através de equipamentos do tipo IoT) (Waedt et al. 2016) (Gaur et al. 2015) (Mijac et al. 2017).

Muitas destas tecnologias de ligação com ou sem fios, dependem de protocolos personalizados e de plataformas de criptografia para assegurar algum nível de segurança. Por outro lado, ainda mais preocupante é o fato de muitas SCs ainda não terem desenvolvido planos de ação para respostas a possíveis ataques cibernéticos aos serviços das cidades, da infraestrutura tecnológica e dos SI/TI (Ijaz et al. 2016). Neste sentido, torna-se importante para as várias áreas ou domínios das SC com suporte a SI/TI assegurar uma arquitetura que reconcilie todos os requisitos de à acessibilidade, disponibilidade, robustez, escalabilidade e segurança dos serviços disponibilizados pelas SC. Waedt, Karl, Ciriello (2016), apresenta um estudo sobre a identificação automática de ativos (equipamentos tecnológicos SI/TI) para as SCs assim como uma abordagem aos requisitos para a avaliação do risco de cibersegurança. O estudo concentrou-se em identificar, descrever e "rastrear" ativos de forma manual e automática, além de atribuir o conceito de TASCs - *Tiered Application Security Controls* que podem beneficiar da gestão abrangente e mais formal dos ativos da infraestrutura tecnológica. Isto inclui a disponibilidade e a integridade dos recursos de SI/TI fixos e móveis ligados a redes com e sem fios, bem como a confiabilidade e a integridade dos ativos de software instalados nos servidores e em ambientes na nuvem (*cloud*). Desta forma, salienta referir as necessárias preocupações sobre a identificação automática de ativos para as SCs como descrições "semi-formais" de ativos, detalhes avançados sobre a relação entre os ativos e a rastreabilidade de modo a reduzir e a mitigar os riscos de vulnerabilidades destes equipamentos.

Khatoun e Sherali (2017) afirmam que a crescente proliferação e instalação de SI/TI na infraestrutura das cidades aumentou o interesse no conceito "SCs", uma vez que se espera que os serviços disponibilizados aos cidadãos melhorem, em última análise, a sua qualidade de vida. Por outro lado, a incorporação das TIC abre várias questões de segurança e privacidade num ambiente de SC, nomeadamente no que diz respeito a infraestruturas críticas, edifícios inteligentes, sistemas de transporte inteligentes, governança eletrónica, saúde digital ou IoT, ou seja, questões de privacidade e modelos de privacidade devem efetivamente ser criados, implementados e monitorizados de modo a mitigar o risco de vulnerabilidades informáticas.

.

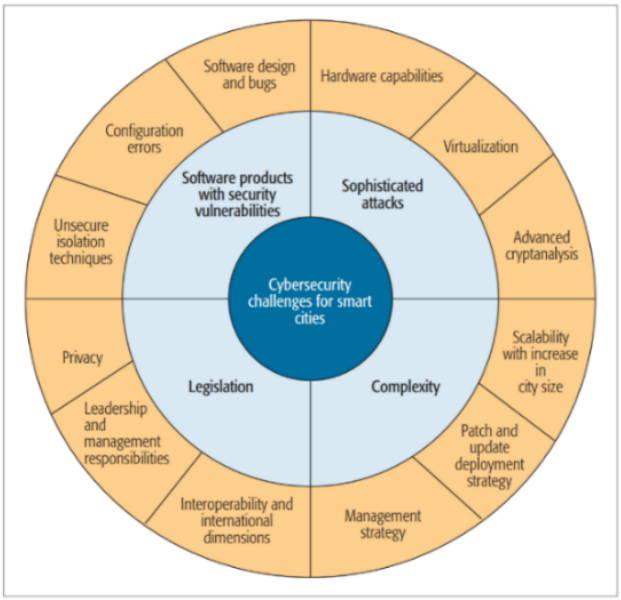


**Figura 2.4 – Ilustração dos desafios a contemplar na Ciber Segurança (Khatoun, e Zeadally, 2017).**

A Figura 2.4 (Khatoun, e Zeadally, 2017) ilustra alguns desafios associados à Cibersegurança para as SC e reflete em geral estudos associados à problemática as SC com a cibersegurança (Lévy-Bencheton e Darr, 2015) (Waedt et al. 2016) (Khatoun e Zeadally, 2017) (Armin et al. 2017) (Zhiyi e Shahidehpour, 2017) (Li e Liao, 2018).

Ao longo dos últimos anos e em paralelo com estas trabalhos de investigação associado às SC e à cibersegurança, a agência da união europeia para segurança de redes e informação [17] tem analisado e apresentado várias orientações para um modelo de arquitetura tecnológica "segura" para a disponibilização e interligação de serviços para pequenas e médias empresas, assim como o relacionamento entre pessoas, processos, informação e tecnologias, indo de encontro aos desafios descritos acima e apresentados em vários artigos

de investigação como é o caso dos trabalhos de Waedt et al (2016), Khatoun e Zeadally (2017) e de Zhang et al. (2017).

No seguimento da análise da problemática associada às SC e à cibersegurança, na secção 2.2 iremos complementar esta informação apresentando um conjunto de orientações, normas e *frameworks* utilizadas para mitigar os riscos e vulnerabilidades da Cibersegurança. Antes disso, iremos descrever a experiência e conhecimento obtido na participação em conferências mundiais sobre estas temáticas e que melhor contribuíram para a realização deste trabalho.

## 2.1. Eventos Tecnológicos Relevantes

Nos últimos anos tem crescido o número de eventos tecnológicos associados às SC, assim como através da aplicabilidade das temáticas da segurança informática e da cibersegurança. No sentido de um melhor enquadramento com as temáticas, tecnologias, sistemas e evoluções tecnológicas, durante a realização deste trabalho de dissertação, participou-se num conjunto de eventos dos quais se salienta as principais temáticas e assuntos abordados, tendo sido selecionados alguns temas considerados relevantes para contribuir para adquirir um maior conhecimento e ser concretizado neste trabalho. :

- **Cybercon 2018 - Atlanta GA, US.** A Cybercon 2018 (decorreu em Sofia, Bulgária, entre 15-16 de Junho de 2018), reuniu líderes empresariais, académicos e governamentais para discutir o cenário da segurança em constante evolução, realçando a cibersegurança como um risco estratégico de negócios corporativos. A conferência foi repleta de sessões e práticas sobre questões de cibersegurança, especialmente os desafios de cibersegurança enfrentados pelos setores financeiros. Foi discutido o fortalecimento da segurança como um CISO pós-ataque. Os CISOs devem aprender a operar dentro da organização com o conhecimento e o entendimento de um CISO pós-ataque, mesmo que ainda não o tenham pessoalmente. Foi discutido a necessidade de avaliar e superar desafios pós-ataque, reengenharia das práticas de segurança e a necessidade de desenvolver e implementar uma estrutura bem-sucedida de governança. Considerou-se que a melhor maneira de proteger uma empresa/SC é ver tudo através de uma lente pós-ataque, o que significa tornar-se um líder de mudança que defende uma cultura de

segurança. Numa das sessões páticas foi vivida uma experiência digital projetada para simular um ataque virtual complexo ocorrida em tempo real. Os participantes da sessão enfrentaram o desafio de tomar boas decisões sob pressão do tempo com fatos incompletos. A Cybercon 2018 ofereceu perspetivas para ajudar os CISOs, profissionais de segurança, empresários e decisores políticos a tomar decisões inteligentes que consideram completamente as questões de cibersegurança como parte integrante do sucesso das organizações.;

- **Cybersecurity, smart cities and critical infrastructure CyberCon 2018**[2] (decorreu em Sofia, Bulgaria, entre 15-16 de Junho de 2018). O objetivo geral deste evento foi apoiar a integração e interação entre órgãos públicos e privados com especialistas em cibersegurança, gestores de infraestruturas críticas, fornecedores de soluções *e-Health* e SC. Nesta conferência foi considerada a necessidade de desenvolver e implementar medidas para tornar a Europa mais confiável e segura online, para que cidadãos e empresas possam usufruir completamente dos benefícios da economia digital. É necessário garantir que a UE possa ser um catalisador do investimento público e privado, com foco em infraestrutura de rede digital de alta qualidade. Foi vastamente discutida a necessidade de aplicar às cidades inteligentes várias tecnologias modernas (arquitetura corporativa, digital, microsserviços, blockchain, coordenação explícita etc.) para alcançar algumas características emergentes desejadas (por exemplo, um alto nível de confiabilidade) de sistemas digitais complexos.
- Security NATO'S Digital Endeavour – Cybersecurity Symposium – NIAS'2018
  Decorreu em Bruxelas entre 16-18 de Outubro de 2018 e teve como objetivo alertar para o mundo virtual de hoje. A cibersegurança é uma parte essencial de todas as operações da NATO, seja em terra, no ar ou no mar, em um ambiente conjunto ou combinado. O NIAS18 abordou a cibersegurança na perspetiva operacional, aplicações cientes e resilientes de Cyber Security e tentou promover a construção,de uma "cyber-workforce". Foi também falado o tema da segurança de uma "workforce" móvel e como se poderá atravessar os limites da "cloud".

- **BlackHat – Europe 2018**[3] (que decorreu em Londres de 3-6 de Dezembro de 2018). O Black Hat Briefings é uma conferência de segurança de computadores que fornece

[2] https://cybercon.eu/
[3] https://www.blackhat.com/eu-18/

consultoria, formação e briefings de segurança a hackers, corporações e agências governamentais em todo o mundo. A conferência ocorre regularmente em Las Vegas, Barcelona, Londres, Abu Dhabi. A Black Hat Briefings reúne profissionais de segurança para falar abertamente sobre as empresas e os governos e dos problema que enfrentam, bem como as soluções para esses problemas. Os diversos tópicos a serem abordados incluiram ciber ataques com motivação política, recuperação de passwords de teclados usando emanações térmicas, ataque do Microsoft Edge e deteção de "falsificações profundas". Além das sessões, outros 30 briefings também foram agendados para o Business Hall, onde os fornecedores analisam segurança de aplicações, proteção de infraestrutura, Gestão de identidade e acesso e muito mais. O Black Hat Europe Arsenal, permite que investigadores e a comunidade de código aberto façam demonstrações ao vivo das ferramentas que desenvolvem e usam nas suas profissões diárias. O arsenal deste ano contou com quase 50 ferramentas que abrangem tópicos que variam de Android e iOS a hackers móveis e a Internet das coisas.

- **CDays 2019 – Porto, Portugal - O C-DAYS 2019**: realizado no Porto, focou-se na segurança digital nas PME, nos desafios emergentes da transformação digital e no reflexo de uma economia cada vez mais absorvida pelo mundo digital. A segurança digital nas PME, os desafios emergentes das mudanças digitais e o reflexo de uma economia cada vez mais absorvida pelo mundo digital estiveram na agenda dos dois dias de trabalho. A necessidade de uma força conjunta para combater as ameaças em potencial neste campo, porque "empresas e cidadãos precisam estar preparados para esses novos desafios: conscientizar e educar; crescer em individualidade e coletividade".
- **Smart Cities Summit 2019 – Lisbon, Portuga**l: Neste evento, foram discutidos os novos desafios para as cidades inteligentes, bem como novas soluções projetadas para melhorar a qualidade de vida das pessoas, criando comunidades mais modernas, eficientes e sustentáveis. Desta cimeira nacional constou, entre outros eventos, uma mesa redonda em que participaram vários autarcas que abordaram as matérias tecnológicas já em utilização nos seus municípios e os desafios que se colocam hoje em dia, cada vez mais exigentes, mantendo-se os mesmos recursos humanos, financeiros e patrimoniais. Por isso, para estes autarcas, o desafio é agarrar a inteligência artificial e, através dela, promover um cada vez melhor desenvolvimento dos territórios. Também foi abordado que as cidades tem potencial para terem um

saldo energético neutro através de uma gestão holística adequada e sistemas seguros a nível informático, colocando o foco na descarbonização e na neutralidade carbónica. Foi abordado que as autarquias tem de dotar as suas infraestruturas de sensores e outros dispositivos conectáveis, para recolher os dados, depois esses dados vão para a *cloud*, e é aqui que a inteligência artificial e a analítica assumem um papel critico na produção de informação útil.

Em termos de análise da participação nestes eventos, assim como as temáticas envolvidas destaca-se como relevante os seguintes aspetos: em todas as conferências, foi salientado que a cooperação é um passo fundamental para a segurança no ciberespaço e as organizações precisam criar o hábito de 'aprender a partilhar' boas práticas, da maneira como lidaram com um evento específico.

Nos últimos anos, testemunhamos um aumento do investimento das organizações em cibersegurança e segurança da informação em geral. Há duas razões principais pelas quais se faz esse investimento: regular e manter a confiança do consumidor/cidadão nas organizações. Em setores mais regulamentados, como o setor financeiro, sempre houve investimentos, no entanto, os reguladores tornaram-se mais exigentes, o que exige que as instituições respondam a esse requisito com medidas mais concretas, preparando-se melhor e não apenas para redigir ou aprovar políticas, mas também para implementar políticas. Em setores menos regulados, a confiança do consumidor/cidadão é a motivação para o investimento.

É possível melhorar a governança da cibersegurança de modo a impulsionar a capacidade de resposta da comunidade internacional a ciber ataques e incidentes e que, ao mesmo tempo, é impossível evitar todos os ataques. Por conseguinte, a rapidez de deteção e resposta e a proteção das infraestruturas de importância critica, em conjunto com a melhoria do intercambio de informações e da coordenação entre os setores publico e privado, são alguns dos principais desafios a superar. Por ultimo, a crescente escassez de competências em matéria de cibersegurança significa que o reforço das competências e da consciencialização em todos os setores e níveis da sociedade é também um desafio fundamental.

## 2.2. Linhas Orientadoras, *Framework*s e *Standards*

Nos últimos anos várias orientações, normas e *frameworks* têm vindo a ser propostas para o desenho, gestão e monitorização da segurança da infraestrutura tecnológica associadas aos SI/TI, como por exemplo a ISO 27001 [18], o COBIT *Information and Technology Control Objectives* [19] assim como algumas orientações para as boas práticas do uso dos SI/TI como o ITIL (*Information Technology Infrastructure Library*) [20]. Por sua vez, vários estudos têm vindo a ser publicados que resumem a problemática destas propostas no âmbito da segurança informática, como por exemplo em Ribeiro et al. (2019).

Por outro lado, a cibersegurança é uma das mais recentes terminologias, salientando desafios e preocupações sobre a segurança em SI/IT e vários trabalhos de investigação têm vindo a ser apresentados como Lévy-Bencheton e Darra (2015), Waedt et al. (2016), Armin et al. (2017), Khatoun e Zeadally (2017) e Zhiyi e Shahidehpour (2017), para referir alguns. Por sua vez, algumas orientações têm vindo a ser propostas através de relatórios de análise e de evidências de precauções e alertas, ou através da disponibilização de *frameworks* para a avaliação do estado de situação das plataformas tecnológicas face aos desafios associados à cibersegurança. Um desses relatórios foi elaborado pelo *Financial Industry Regulatory Authority* dos Estados Unidos da América (EUA) [21] que apresenta um conjunto de considerações que as empresas se podem basear para elaborar os seus programas de segurança informática associados à cibersegurança. O *Institute of Standards and Technology* (NIST) dos EUA, apresenta uma *framework* -*Cybersecurity Framework of the United States National* [22].

O Instituto SANS - *Critical Security Controls for Effective Cyber Defense* [23] é uma organização privada com fins lucrativos que oferece formação e certificação em segurança da informação e cibersegurança. O Instituto foi fundado em 1989 como uma cooperativa dedicada à pesquisa e educação em segurança de TI. O SANS mantém o maior repositório de informações de segurança do mundo e também é o maior organismo de certificação. A organização disponibiliza gratuitamente uma grande coleção de documentos de pesquisa de segurança e é responsável por um sistema de aviso da Internet: o *Internet Storm Center*.

O programa GIAC (*Global Information Assurance Certification*) do Instituto SANS fornece um meio baseado em padrões para garantir o conhecimento e as capacidades de um profissional de segurança.

A ISO 27001 (Gestão da Segurança da Informação) e a nova ISO 27032 - *Information technology — Security techniques — Guidelines for cybersecurity* [24] evidencia a atualização da preocupação de definir guias e standards associados para a cibersegurança. Trata-se ainda de uma primeira versão da norma que define orientações gerais a ter em consideração na análise da aplicabilidade e em atenção nos SI/TI da infraestrutura tecnológica de suporte aos serviços.

Por outro lado, o objetivo do Projeto OWASP *Open Cyber Security Framework* [25] é criar um quadro prático para a cibersegurança Atualmente, existem algumas estruturas do NIST (*Cyber Security Systems Framework)* ou da ISACA, por exemplo, e outras estruturas pagas ou locais, mas não existe uma estrutura aberta que qualquer governo ou organização possa adotar. Criar, implementar e gerir uma *Cybersecurity Framework* tornou-se uma necessidade (ou pode ser uma obrigação) para muitos governos e organizações. O *Open Framework Cybersecurity Framework Project* (OCSFP) é um projeto aberto dedicado a permitir que as organizações concebam ou aprimorem uma *Cybersecurity Framework*. Todas as informações no OCSFP são gratuitas e abertas a qualquer pessoa. Todos são convidados a participar e colaborar para melhorar e disponibilizar.

Neste contexto, de uma forma direta e indireta, estas orientações, normas e *frameworks* foram estudadas e aplicadas neste trabalho. Trata-se efetivamente de um vasto conjunto de indicações que os intervenientes na disponibilização de serviços digitais devem ter em conta face à segurança cibernética, quer sejam cidadãos, empresas, instituições púbicas e privadas, sendo ainda mais importante esta questão da mitigação dos riscos da segurança cibernética quando aplicada a SC.

## 2.3. Estudos Reais de Aplicabilidade Cidades Inteligentes- Cibersegurança

Em Krishnan et al. (EY, 2018) [26], pode-se encontrar um bom relatório sobre a relação entre SCs e cibersegurança, que identifica uma série de desafios, vulnerabilidades, riscos potenciais e uma categorização de serviços inteligentes com base em riscos, nomeadamente vulnerabilidades e seu impacto. O mesmo relatório descreve várias iniciativas importantes de Cibersegurança adotadas em todo o mundo, nomeadamente nas cidades dos Estados Unidos da América (Lei de Melhoria da Cibersegurança, 2017, *Cyber Security Systems Framework* 1.0 (NIST), Diretrizes de Cibersegurança para Segurança de Sistemas Inteligentes), *Nova York Secure Initiative*, Plano Nacional de Proteção de Infraestrutura como Parceiro de Segurança e Resiliência de Infraestruturas Críticas, *Cyber Lab* em Los

Angeles); na Europa (Política de Segurança da Rede e Segurança da Informação da União Europeia para Vigilância Setorial, Estrutura de Certificação de Equipamentos, Recomendações de Segurança para a Internet das Coisas (IoT), Agência da União Europeia para Diretrizes de Rede e Segurança da Informação em Cibersegurança para Cidades Inteligentes, Programa de Análise para a Segurança de infra-estruturas críticas); em Singapura (Lei de Cibersegurança de Singapura, 2018, Lei de Proteção de Dados, Padrões do Ecossistema da Internet das Coisas, Laboratório Nacional de Pesquisa e Desenvolvimento de Cibersegurança, Centro de Inicialização para Cibersegurança) e na Austrália (Aliança da Internet das Coisas, Austrália, Políticas e Melhores Práticas de Cidades Inteligentes, Programa de Análise e Modelagem de Infraestrutura Crítica, Rede de Intercâmbio de Informações Confiáveis).

Em [12], a KPMG (2019) apresentou um relatório de Cibersegurança nos SCs, descrevendo a estrutura principal para a configuração de componentes de cibersegurança e a necessidade de padrões, trazendo um conjunto de critérios e práticas de cibersegurança como NIST e ISO. Introduzir uma série de medidas-chave para enfrentar os desafios da cibersegurança e do ecossistema SC, ou seja, criar uma estrutura formal de cibersegurança, aumentar a segurança desde o início, usar a segurança de maneira integrada em todos os valores, criar um ambiente virtual e confiável e envolvimento de grupos setoriais, de conhecimento e reguladores para padronizar medidas de segurança. Em [27], o governo indiano apresentou uma estrutura de Cibersegurança que contém boas diretrizes bem estruturadas que consideram o ecossistema de SC quando estão ligadas à cibersegurança.

Após essa revisão da literatura e os relatórios apresentados não apenas acima, mas também na seção de referência, é possível definir um questionário (ou lista de verificação) para avaliar a cibersegurança em uma cidade inteligente.

Neste contexto, apresentamos evidências da aplicabilidade da cibersegurança às SC em cidades mundiais. Salientam-se os desafios e a problemática associada à segurança cibernética que deverá ser mitigada e reduzir os riscos de exposição das vulnerabilidades da infraestrutura tecnológica disponibilizada pelos serviços das SC. Complementarmente a esta informação destes relatórios de consultoras de renome internacional e de entidades governamentais, outra vasta informação apresentada na secção da bibliografia e referências bibliográficas evidencia esta problemática, assim como alguns casos de estudo e de investigação.

## 2.4. Proposta de Lista de Verificação do Estado da Relação da Cibersegurança nas Cidades Inteligentes

Neste trabalho, foram seguidas as regras do setor financeiro (*USA Financial industry*) [21] e as orientações e listas de verificação do Instituto Nacional de Padrões e Tecnologias (NIST), *Cybersecurity Framework* [22], SANS *Critical Security Controls for Effective Cyber Defense* [23], ISO 27001 e 27032 [18, 24] e OWASP *Open Cyber Security Framework Project* [25].

Na lista de verificação seguinte apresenta-se a lista de documentos que deverão ser tidos em consideração para cada subcategoria.

**Tabela 2.1 – Lista de Verificação do controlo do estado da cibersegurança de uma SC – Orientações**

| Function | Domains or Category | Subcategory/Checklist items/Document Orientations |
|---|---|---|
| Identify | Asset Management | **Physical devices and systems** (*NIST SP 800-53 Rev. 4 CM-8, SO/IEC 27001:2013 A.8.1.1, A.8.1.2 , COBIT 5 BAI09.01, BAI09.02*), **Software platforms and applications** (*NIST SP 800-53 Rev. 4 CM-8, ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, COBIT 5 BAI09.01, BAI09.02, BAI09.05*), **Organizational communication and data flows are mapped** (*NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8, ISO/IEC 27001:2013 A.13.2.1 , COBIT 5 DSS05.02*), **External information systems** (*NIST SP 800-53 Rev. 4 AC-20, SA-9, ISO/IEC 27001:2013 A.11.2.6, COBIT 5 APO02.02*), **Electronic Resources** (*NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, ISO/IEC 27001:2013 A.8.2.1, COBIT 5 APO03.03, APO03.04, BAI09.02*), **Cybersecurity roles and responsibilities** (*NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11, ISO/IEC 27001:2013 A.6.1.1, COBIT 5 APO01.02, DSS06.03*). |
| | Business Environment | **Organization's role** (*NIST SP 800-53 Rev. 4 CP-2, SA-12, ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2, COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05*), **Organization's place in critical infrastructure** (*NIST SP 800-53 Rev. 4 PM-8, COBIT 5 APO02.06, APO03.01*), **Priorities for organizational mission** (*NIST SP 800-53 Rev. 4 PM-11, SA-14, COBIT 5 APO02.01, APO02.06, APO03.01*), **Dependencies and critical functions** (*NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14, ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3*), **Resilience requirements** (*ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1, NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14, COBIT 5 DSS04.02*) |
| | Governance | **Organizational information security policy** (*NIST SP 800-53 Rev. 4 -1 controls from all families, ISO/IEC 27001:2013 A.5.1.1, COBIT 5 APO01.03, EDM01.01, EDM01.02*), **Information security roles** (*NIST SP 800-53 Rev. 4 PM-1, PS-7, ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, COBIT 5 APO13.12*), **Legal and regulatory requirements** (*NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1), ISO/IEC 27001:2013 A.18.1, COBIT 5 MEA03.01, MEA03.04*), **Governance and risk Management processess** (*NIST SP 800-53 Rev. 4 PM-9, PM-11, COBIT 5 DSS04.02*). |
| | Risk Assessment | **Asset vulnerabilities** (*NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, ISO/IEC 27001:2013 A.12.6.1, A.18.2.3, COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04*), **Threat and vulnerability information** (*NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5, ISO/IEC 27001:2013 A.6.1.4*), **Threats management** (*NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16, COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04*), **Potential business impacts** (*NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14, COBIT 5 DSS04.02*), **Threats vulnerabilities to determine risk** (*NIST SP 800-53 Rev. 4 RA-2, ISO/IEC 27001:2013 A.12.6.1, COBIT 5 APO12.02*), **Risk responses** (*NIST SP 800-53 Rev. 4 PM-4, PM-9, COBIT 5 APO12.05, APO13.02*). |
| | Risk Management Strategy | **Risk management processes** (*NIST SP 800-53 Rev. 4 PM-9, COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02*), **Organizational risk tolerance** (*NIST SP 800-53 Rev. 4 PM-9, COBIT 5 APO12.06*), **Dissemination of organization's determination of risk tolerance** (*NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14*). |
| Protect | Access Control | **Identities and credentials** (*NIST SP 800-53 Rev. 4 AC-2, IA Family, ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, COBIT 5 DSS05.04, DSS06.03*), **Physical access to assets** (*NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE5, PE-6, PE-9, ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, COBIT 5 SS01.04, DSS05.05*), **Remote access** (*NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20, ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1, COBIT 5 APO13.01, DSS01.04, DSS05.03*), **Access permissions** (*NIST* |

| Function | Domains or Category | Subcategory/Checklist items/Document Orientations |
|---|---|---|
| | | *SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16, ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4*), **Network integrity** (*NIST SP 800-53 Rev. 4 AC-4, SC-7, ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1*). |
| | Awareness and Training (urr-understand roles & responsibilities | **All users are informed and trained** (*NIST SP 800-53 Rev. 4 AT-2, PM-13, ISO/IEC 27001:2013 A.7.2.2, COBIT 5 APO07.03, BAI05.07*), **Privileged users urr** (*NIST SP 800-53 Rev. 4 AT-3, PM-13, ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, COBIT 5 APO07.02, DSS06.03*), **Third-party stakeholders urr** (*NIST SP 800-53 Rev. 4 PS-7, SA-9, ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, COBIT 5 APO07.03, APO10.04, APO10.05*), **Senior executives urr** (*NIST SP 800-53 Rev. 4 AT-3, PM-13, ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2*), **Physical and information security personnel urr** (*NIST SP 800-53 Rev. 4 AT-3, PM-13, ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, COBIT 5 APO07.03*). |
| | Data Security | **Data-at-rest is protected** (*NIST SP 800-53 Rev. 4 SC-28, ISO/IEC 27001:2013 A.8.2.3, COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06*), **Data-in-transit is protected** (*NIST SP 800-53 Rev. 4 SC-8, ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3, COBIT 5 APO01.06, DSS06.06*), **Assets are formally managed** (*NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16, ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7, COBIT 5 BAI09.03*), **Adequate capacity** (*NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5, ISO/IEC 27001:2013 A.12.3.1, COBIT 5 APO13.01*), **Protections against data leaks** (*NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4), ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3, COBIT 5 APO01.06*), **Integrity checking mechanisms** (*NIST SP 800-53 Rev. 4 SI-7, ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3*), **The development and testing environment(s) are separate from the production environment** (*NIST SP 800-53 Rev. 4 CM-2, ISO/IEC 27001:2013 A.12.1.4, COBIT 5 BAI07.04*). |
| | Information Protection Processes and Procedures (Security policies) | **A baseline configuration of information technology** (*NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10, ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05*), **A System Development Life Cycle to manage systems is implemented** (*NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA10, SA-11, SA-12, SA-15, SA-17, PL-8, ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5, COBIT 5 APO13.01*), **Configuration change control processes are in place** (*NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10, ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, COBIT 5 BAI06.01, BAI01.06*), **Backups of information are conducted, maintained, and tested periodically** (*NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9, ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3, COBIT 5 APO13.01*), **Policy and regulations for organizational assets are met** (*COBIT 5 APO13.01, ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, COBIT 5 DSS01.04, DSS05.05*), **Data is destroyed according to policy** (*NIST SP 800-53 Rev. 4 MP-6, ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, COBIT 5 BAI09.03*), **Protection processes are continuously improved** (*NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6, COBIT 5 APO11.06, DSS04.05*), **Effectiveness of protection technologies is shared with appropriate parties** (*NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4, ISO/IEC 27001:2013 A.16.1.6*), **Response plans are in place and managed** (*NIST SP 800-53 Rev. 4 CP-2, IR-8, ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 COBIT 5 DSS04.03*), **Response and recovery plans are tested** (*NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14, ISO/IEC 27001:2013 A.17.1.3*), **Cybersecurity is included in human resources practices** (*NIST SP 800-53 Rev. 4 PS Family, ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4, COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05*), **A vulnerability management plan is developed and implemented** (*NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2, ISO/IEC 27001:2013 A.12.6.1, A.18.2.2*). |
| | Maintenance | **Maintenance and repair of organizational assets** (*NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, COBIT 5 BAI09.03*), **Remote maintenance of organizational assets is approved logged, and performed in a manner that prevents unauthorized access** (*NIST SP 800-53 Rev. 4 MA-4, ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1, COBIT 5 DSS05.04*). |
| | Protective Technology | **Audit/log records are determined** (*NIST SP 800-53 Rev. 4 AU Family*), **documented, implemented, and reviewed in accordance with policy** (*ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, COBIT 5 APO11.04*), **Removable media is protected and its use restricted according to policy** (*NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7, ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9, COBIT 5 DSS05.02, APO13.01*), **Access to systems and assets is controlled, incorporating the principle of least functionality** (*NIST SP 800-53 Rev. 4 AC-3, CM-7, ISO/IEC 27001:2013 A.9.1.2, COBIT 5 DSS05.02*)**, Communications and control networks are protected** (*NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, COBIT 5 DSS05.02, APO13.01*). |
| Detect | Anomalies and Events | **A baseline of network operations and expected data flows** (*NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4, COBIT 5 DSS03.01*), **Detected events are analyzed** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.16.1.1, A.16.1.4*), **Event data are aggregated and correlated from multiple sources and sensors** (*NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR5, IR-8, SI-4*), **Impact of events is determined** (*NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4, COBIT 5 APO12.06*), **Incident alert thresholds are established** (*NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4, COBIT 5 DSS05.07*). |

| Function | Domains or Category | Subcategory/Checklist items/Document Orientations |
|---|---|---|
| | Security Continuous Monitoring | **The network is monitored to detect potential cybersecurity events** (*NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4, COBIT 5 DSS05.07*), **The physical environment is monitored to detect potential cybersecurity events** (*NIST SP 800-53 Rev. 4*), **Personnel activity is monitored to detect potential cybersecurity events** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.12.4.1*), **Malicious code is detected** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.12.2.1, COBIT 5 DSS05.01*), **Unauthorized mobile code is detected** (*NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44, ISO/IEC 27001:2013 A.12.5.1*), **External service provider activity is monitored** (*NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA9, SI-4, ISO/IEC 27001:2013 A.14.2.7, A.15.2.1, COBIT 5 APO07.06*), **Monitoring for unauthorized personnel, connections, devices, and software is performed** (*NIST SP 800-53 Rev. 4*), **Vulnerability scans are performed** (*NIST SP 800-53 Rev. 4 RA-5, ISO/IEC 27001:2013 A.12.6.1, COBIT 5 BAI03.10*). |
| | Detection Processes | **Roles and responsibilities for detection are well defined** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.6.1.1, COBIT 5 DSS05.01*), **Detection activities comply with all applicable requirements** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.18.1.4*), **Detection processes are tested** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.14.2.8, COBIT 5 APO13.02*), **Event detection information is communicated to appropriate parties** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.16.1.2, COBIT 5 APO12.06*), **Detection processes are continuously improved** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.16.1.6, ISO/IEC 27001:2013 A.16.1.6*). |
| Respond | Response Planning | **Response plan is executed** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.16.1.5, COBIT 5 BAI01.10*) |
| | Communications | **Personnel know their roles and order of operations when a response is needed** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.6.1.1, A.16.1.1*), **Events are reported consistent with established criteria** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.6.1.3, A.16.1.2*), **Information is shared consistent with response plans** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.16.1.2*), **Coordination with stakeholders occurs consistent with response plans** (*NIST SP 800-53 Rev. 4*), **Voluntary information sharing occurs with external stakeholders** (*NIST SP 800-53 Rev. 4*). |
| | Analysis | **Notifications from detection systems are investigated** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5, COBIT 5 DSS02.07*), **The impact of the incident is understood** (*NIST SP 800-53 Rev. 4 CP-2, IR-4, ISO/IEC 27001:2013 A.16.1.6*), **Forensics are performed** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.16.1.7*), **Incidents are categorized** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.16.1.4*). |
| | Mitigation | **Incidents are contained** (*NIST SP 800-53 Rev. 4 I, ISO/IEC 27001:2013 A.16.1.5*), **Incidents are mitigated** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.12.2.1, A.16.1.5*), **Newly identified vulnerabilities are mitigated** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.12.6.1*). |
| | Improvements | **Response plans incorporate lessons learned** (*NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013 A.16.1.6, COBIT 5 BAI01.13*), **Response strategies are updated** (*NIST SP 800-53 Rev. 4*). |
| Recover | Recovery Planning | **Recovery plan is executed during or after an event** (NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013). |
| | Improvements | **Recovery plans incorporate lessons learned** (*NIST SP 800-53 Rev. 4, COBIT 5 BAI05.07*), **Recovery strategies are updated** (*NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8, COBIT 5 BAI07.08*). |
| | Communications | **Public relations are managed** (*COBIT 5 EDM03.02*), Reputation after an event is repaired (COBIT 5 MEA03.02), **Recovery activities are communicated** (*NIST SP 800-53 Rev. 4*). |

Nesta seção apresentamos a lista de verificação do controlo do estado da cibersegurança de uma SC, em particular as orientações a serem seguidas (ex.: para a função "*Identify*" e o domínio "*Asset Management*" e para a subcategoria "*Software platforms and applications*", devem ser seguidas as orientações: NIST SP 800-53 Rev. 4 CM-8, ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, COBIT 5 BAI09.01, BAI09.02, BAI09.05), assim como as questões a colocar na avaliação do estado da cibersegurança quando aplicada à infraestrutura tecnológica de uma SC.

Estas orientações poem ser encontradas nos seguintes links:

- **Control Objectives for Information and Related Technology (COBIT):** http://www.isaca.org/COBIT/Pages/default.aspx

- **Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC):** http://www.counciloncybersecurity.org
- **ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program**: http://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisplay.cfm&ProductID=10243
- **ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels:** http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=13420
- **ISO/IEC 27001, Information technology -- Security techniques - Information security management systems - Requirements:** http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534
- **NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations**. http://dx.doi.org/10.6028/NIST.SP.800- 53r4.

Seguindo a estrutura da tabela 2.1 e para cada subcategoria, apresentam-se as questões propostas a colocar na avaliação do estado da cibersegurança quando aplicada à infraestrutura tecnológica de uma SC, nomeadamente nas subcategorias mencionadas no Anexo-C-NIST-CS-ML

As questões propostas neste trabalho encontram-se no ficheiro em anexo denominado como Anexo-C-NIST-CS-ML na folha "SC" coluna "E". Através das respostas a estas perguntas usando os cinco níveis de maturidade indicados no mesmo anexo os decisores poderão avaliar o nível de maturidade ao nível de políticas / praticas.

Com base nesta informação, a mesma foi testada num caso de estudo que se apresenta na secção seguinte, no sentido de avaliar a cibersegurança de uma SC e, de alguma forma, responder à questão da investigação: "A cibersegurança é um pilar necessário das Smart Cities?".

# 3. Caso de Estudo

## 3.1. Contextualização

O objetivo deste trabalho é realizar uma avaliação de Cibersegurança (usando um questionário ou lista de verificação proposta) para uma verdadeira infraestrutura tecnológica de SC, ou seja, avaliar seu nível de maturidade, garantir a segurança e a privacidade digital. O caso de estudo é de uma CS portuguesa, do Norte, considerada de nível médio de acordo com a estrutura dos domínios da SC apresentada na Tabela 3.1.

Por motivos de confidencialidade o nome do município não é mencionado neste documento, mas sim noutros ou noutras apresentações efetuadas pelo autor deste trabalho. A estrutura da caracterização da SC é dividida em pilares estratégicos, cada um com uma orientação estratégica e linhas estratégicas. A cada um desses pontos é atribuída uma série de vetores estratégicos com base em um conjunto de fatores (por exemplo, promovendo as competências das pessoas para melhorar a qualidade de vida; o desenvolvimento da dimensão humana no contexto de abertura à diversidade e ao multiculturalismo; capital cultural local e regional e promoção da sua transformação em fatores de qualificação; melhoria da qualidade de vida e promoção das artes e da criatividade).

Assim, a cada objetivo é atribuído um conjunto de projetos de políticas do município local com base na estratégia 2020-2030 (com ou sem intervenção em TIC) e um conjunto de indicadores de avaliação da maturidade da cidade inteligente da União Europeia [15]. Após este mapeamento entre elementos e vetores estratégicos, o mapeamento dos domínios da SC no contexto das TIC foi analisado e as diretrizes e melhores práticas para uma melhor governança local são estabelecidas para assegurar o melhor relacionamento entre Cibersegurança e a SC.

**Tabela 3.1 – Caracterização em grelha da Smart City em estudo**

| Strategic Pillars | Strategic Directions | Strategic Line | Strategic Vectors | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | a | b | c | d | e | f | g | h | i |
| Society (intelligent people) and Quality of life | Smart Education | e-Education (e.g. Video Conference) | | | | x | x | | | | x |
| | | School Digital Solutions | | | | x | x | | | | x |
| | | Training and Individuals's Capacity | | | | x | x | | | | x |
| | Smart Citizen - Creativity | | | x | | | | x | | x | |
| | Smart Citizen - Inclusion | Integration of Migrants, Reduced Mobility | | x | | | x | | x | | x |
| | | Inclusion of people with physical and cognitive difficulties | | x | | | x | | | | X |
| | Smart Health | Telemedicine and Remote Monitoring | | x | | | x | | | | x |
| | | Promotion of Healthy Actions and Habits | | x | | | x | | | | x |
| | Smart Security and Safety | Legislative Reinforcement | x | | | | | | | | x |
| | | Emergency Response | x | | | | | | x | | x |
| | | Intelligent street lighting and Monitoring of "Video Crime" | | | | | | | x | x | x |
| | | Integration and control of electronic devices | x | | | | | | x | | x |
| | Smart Citizen - Hospitality | | x | x | x | | x | | | | x |
| | Green Buildings | Providing requalified and modern infrastructures | x | | x | | | | | x | x |
| | | Availability of modernized / new infrastructures | x | | x | | | | | x | x |
| | Smart Citizen - Culture and wellness | Qualification and Social Inclusion | x | x | x | x | x | x | | x | x |
| Environment | Smart Management | Smart Agriculture | x | | x | | | | | x | x |
| | Sustainable Smart Buildings | Sustainable Buildings and Urbanism | x | | x | | | | | x | x |
| | Resource Mangement | | x | | x | | | | | x | x |
| | Sustainability | | x | | x | | | | | x | x |
| Economy | Productivity/ Incubation / Coworking | | x | | | x | x | | x | | x |
| | Local and global link economy | Smart Agriulture and Smart Local/Global Links | x | x | x | | | | x | | x |
| | Economic Agents | Exchange development and e-commerce | x | x | | | x | | x | | |
| Smart Governance | Digital Transformation | Complaint Management; Various forms of payment; | x | | | | x | | | | x |
| | | Electronic Services | | | | | | | | | x |
| | e-Governance | | x | x | x | | | | | | x |
| | Civil Protection | Efficient Management of Public Processes | x | | x | | | | x | | x |
| | | Infrastructures of the city | x | | | | | x | x | | x |
| | Commitment | Commitment to the citizen and with the industry | x | | | | | x | x | | x |
| | Incubation / Coworking | | x | | | x | x | | | | x |
| Smart Mobility | Support Infrastructures | Improving Infrastructures | x | x | x | | | | x | x | x |
| | Control of Access to Areas of the City | | | | | | | | x | x | x |
| | Smart Parks | Efficient Parking Management | | | x | | x | | x | x | |
| | Intelligent Traffic Management | Creation of Parking Parks and efficient traffic monitoring | | | x | | x | | x | x | |
| | Multi-Modal Transport Integration | Integrated data collection platform for means of transport to support integrated transport (buses, bicycles, trains, etc.) | | | x | | x | | x | x | |
| | Efficient Urban Mobility Solutions | Electric buses, sharing of electric bicycles; Cycle tracks, pedestrian lanes, promotion of policies for the use of means of transport. | x | x | x | | x | | x | x | |
| Smart Infrastructures | Regeneration / Creation of Urban Infrastructures | Urban Regeneration | x | x | | | | | | x | x |
| | | Modernization / Creation of Infrastructures | x | x | x | | | | | x | x |
| | Water, Noise and Air | Smart Meter | x | | x | | | | | | X |
| | | Renewable Energy Sources and Efficiency | x | | x | | | | | | x |
| | | Smart Water Grid and Water quality | x | | x | | | | | | x |
| | | Identification of Leaks | x | | x | | | | | | x |
| | | Preventive maintenance | x | | | | | | x | | x |
| | Waste | Waste for Compost ("biological fertilizers") | x | | x | | | | | | x |
| | | Reuse | x | | x | | | | | | x |
| | | Recycle, Treatment and Reduce Waste | x | | x | | | | | | x |
| | Smart Energy | Renewable Energy Sources | x | | x | | | | | x | |
| | | Smart Meter | x | | x | | | | | | x |
| | | Green Buildings and Intelligent Building Construction | x | x | x | | | x | | | |
| | Smart Technology | Internet Of Things | x | x | x | | | | x | | x |
| | | Wireless and Optical fiber | x | x | x | x | x | x | x | x | x |
| | | Communications Infrastructure - Monitoring | x | x | | x | | x | x | | X |
| | Data | Security, Data Protection and Privacy | x | x | | x | | x | x | | x |
| | | Big Data and Open Data | x | x | | x | | x | x | | x |

Legenda:

(a) - “Clusters” e linhas económicas estratégicas e outros setores;

(b) - turismo;

(c) - área rural;

(d) - Emprego e formação;

(e) - coesão social;

(f) - Cultura, identidade e criatividade;

(g) - Conectividade interna e externa;

(h) - Revitalização ou urbana; Reabilitação e Animação;

(i) - Cooperação e Governança.

## 3.2. Aplicabilidade

Neste trabalho, foram seguidas as regras do setor financeiro [21] e as diretrizes e listas de verificação do Instituto Nacional de Padrões e Tecnologias (NIST), Cibersecurity Framework [22], SANS Critical Security Controls for Effective Cyber Defense [23], ISO 270xx [18, 24], e OWASP Open Cyber Security Framework Project [22].

**Tabela 3.2 – Associação dos domínios da lista de verificação da Cibersegurança aos domínios das Cidades inteligentes**

| Function | Domains or Category | Subcategory/Checklist items | SMART city pillar |
|---|---|---|---|
| Identify | Asset Management | Physical devices and systems, Software platforms and applications, Organizational communication and data flows are mapped, External information systems, Electronic Resources, Cybersecurity roles and responsibilities. | Energy Technology Security |
| | Business Environment | Organization’s role, Organization’s place in critical infrastructure, Priorities for organizational mission, Dependencies and critical functions, Resilience requirements. | Energy Mobility Technology Security |
| | Governance | Organizational information security, Information security roles, Legal and regulatory requirements, Governance and risk Management processess. | Governance Technology Security |
| | Risk Assessment | Asset vulnerabilities, Threat and vulnerability information, Threats management, Potential business impacts, Threats vulnerabilities to determine risk, Risk responses. | Infrastructure Technology Security |
| | Risk Management Strategy | **Risk management processes**, **Organizational risk tolerance**, **Dissemination of organization’s determination of risk tolerance**. | Technology Security |
| Protect | Access Control | **Identities and credentials**, **Physical access to assets**, **Remote access**, **Access permissions**, **Network integrity**. | Infrastructure Citizen Technology Security |
| | Awareness and Training (urr-understand roles & responsibilities | All users are informed and trained, Privileged users urr, Third-party stakeholders urr, Senior executives urr, Physical and information security personnel urr. | Education Citizen Technology Security |

| Function | Domains or Category | Subcategory/Checklist items | SMART city pillar |
|---|---|---|---|
| | Data Security | Data-at-rest is protected, Data-in-transit is protected, Assets are formally managed, Adequate capacity, Protections against data leaks, Integrity checking mechanisms, The development and testing environment(s) are separate from the production environment. | Infrastructure Technology Security |
| | Information Protection Processes and Procedures (Security policies) | A baseline configuration of information technology, A System Development Life Cycle to manage systems is implemented, Configuration change control processes are in place, Backups of information are conducted, maintained, and tested periodically, Policy and regulations for organizational assets are met, Data is destroyed according to policy, Protection processes are continuously improved, Effectiveness of protection technologies is shared with appropriate parties, Response plans are in place and managed, Response and recovery plans are tested, Cybersecurity is included in human resources practices, A vulnerability management plan is developed and implemented. | Technology Security |
| | Maintenance | Maintenance and repair of organizational assets, Remote maintenance of organizational assets is approved logged, and performed in a manner that prevents unauthorized access. | Energy Buildings Infrastructure Technology Security |
| | Protective Technology | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy, Removable media is protected and its use restricted according to policy, Access to systems and assets is controlled, incorporating the principle of least functionality, Communications and control networks are protected. | Infrastructure Technology Security |
| Detect | Anomalies and Events | A baseline of network operations and expected data flows, Detected events are analyzed, Event data are aggregated and correlated from multiple sources and sensors, Impact of events is determined, Incident alert thresholds are established. | Infrastructure Technology Security |
| | Security Continuous Monitoring | The network is monitored to detect potential cybersecurity events, The physical environment is monitored to detect potential cybersecurity events, Personnel activity is monitored to detect potential cybersecurity events, Malicious code is detected, Unauthorized mobile code is detected, External service provider activity is monitored, Monitoring for unauthorized personnel, connections, devices, and software is performed, Vulnerability scans are performed. | Infrastructure Technology Security |
| | Detection Processes | Roles and responsibilities for detection are well, Detection activities comply with all applicable requirements, Detection processes are tested, Event detection information is communicated to appropriate parties, Detection processes are continuously improved. | Infrastructure Technology Security |
| Respond | Response Planning | Response plan is executed. | Technology Security |
| | Communications | Personnel know their roles and order of operations when a response is needed, Events are reported consistent with established criteria, Information is shared consistent with response plans, Coordination with stakeholders occurs consistent with response plans, Voluntary information sharing occurs with external stakeholders. | Infrastructure Technology Security |
| | Analysis | Notifications from detection systems are investigated, The impact of the incident is understood, Forensics are performed, Incidents are categorized. | Infrastructure Technology Security |
| | Mitigation | Incidents are contained, Incidents are mitigated, Newly identified vulnerabilities are mitigated. | Infrastructure Technology Security |
| | Improvements | Response plans incorporate lessons learned, Response strategies are updated. | Infrastructure Technology Security |
| Recover | Recovery Planning | Recovery plan is executed during or after an event. | Technology Security |
| | Improvements | Recovery plans incorporate lessons learned, Recovery strategies are updated. | Infrastructure Technology |
| | Communications | Public relations are managed, Recovery activities are communicated. | Infrastructure Technology Security |

A tabela 3.2 apresenta uma série de subcategorias (atribuídas como uma lista de verificação) que foram aplicadas à infraestrutura tecnológica de uma SC em Portugal. Para cada subcategoria, foram seguidas as orientações do NIST [20], ISO 270032 [21] e COBIT [9] e incluídas as informações / pontos do OWASP [25]. Para planear e gerir a infraestrutura de segurança tecnológica, a lista de verificação de Cibersegurança foi complementada com outra baseada nas diretrizes do COBIT, nas melhores práticas de ITIL e na abordagem metodológica ISO 27001 e 27005, além de uma pesquisa baseada em diferentes áreas gerais (áreas de segurança, software), backups, hardware e condições de infraestrutura. A segunda

pesquisa foi subdividida em 156 questões divididas em catorze áreas, apresentadas em [22], ou seja, organização e política, gestão de ativos, recursos humanos, segurança física, proteção ambiental, segurança de dispositivos, gestão de operações, troca de dados, monitorização e registro, controle de auditoria, computação móvel, teletrabalho, teste de vulnerabilidades, gestão de incidentes, continuidade e conformidade dos negócios.

## 3.3. Avaliação e Discussão

Para quantificar o estado da infraestrutura de segurança, o questionário (Anexo-C-NIST-CS-ML) foi preenchida três vezes em três meses e em uma ordem probabilística fora desses períodos.

Numa primeira análise, pode-se afirmar que a cibersegurança é uma das bases mais importantes para analisar a segurança de infraestrutura e serviços digitais em tecnologias inteligentes e pilares de segurança inteligentes. Seguindo essa metodologia de avaliação, somos capazes de representar e quantificar o desempenho da infraestrutura durante um tempo específico e reajustar e verificar alguns problemas e correções a serem alcançadas na infraestrutura.

Na figura 3.1 ilustra-se o resultado de uma simulação aplicada à SC em questão tendo em consideração a lista de verificação e a Cibersergurança da infraestrutura tecnológica da SC.

Com base nas respostas obtidas e de modo a ter uma visão global do estado de maturidade alem dos valores para cada um dos itens é gerado um gráfico (figura 3.2).

Na figura 3.2 ilustra-se os dados obtidos na simulação da lista de verificação do estado de maturidade da SC face á segurança. Como referência foi colocado o valor 3 como valor aceitável (valores de 1 a 5, podendo ser outro intervalo consoante a ponderação do administrador da infraestrutura tecnológica). Neste sentido o Policy Score foi baseado no nível de criticidade adequado para a entidade em questão e o Practice Score como o nível em que se encontra.

| | NIST CSF Categories | Target Score | 2019 Policy Score | 2019 Practice Score |
|---|---|---|---|---|
| | **Overall** | **3,00** | **4,04** | **2,90** |
| IDENTIFY (ID) | Asset Management (ID.AM) | 3,00 | 3,40 | 2,68 |
| | Business Environment (ID.BE) | 3,00 | 3,20 | 2,40 |
| | Governance (ID.GV) | 3,00 | 3,69 | 2,54 |
| | Risk Assessment (ID.RA) | 3,00 | 4,18 | 2,65 |
| | Risk Management Strategy (ID.RM) | 3,00 | 3,86 | 2,57 |
| | Supply Chain Risk Management (ID.SC) | 3,00 | 3,60 | 2,60 |
| PROTECT (PR) | Identity Management, Authentication and Access Control (PR.AC) | 3,00 | 4,33 | 3,78 |
| | Awareness and Training (PR.AT) | 3,00 | 3,43 | 2,43 |
| | Data Security (PR.DS) | 3,00 | 4,25 | 3,38 |
| | Information Protection Processes and Procedures (PR.IP) | 3,00 | 4,25 | 3,25 |
| | Maintenance (PR.MA) | 3,00 | 4,50 | 4,50 |
| | Protective Technology (PR.PT) | 3,00 | 4,40 | 3,00 |
| DETECT (DE) | Anomalies and Events (DE.AE) | 3,00 | 4,00 | 2,20 |
| | Security Continuous Monitoring (DE.CM) | 3,00 | 4,00 | 2,38 |
| | Detection Processes (DE.DP) | 3,00 | 4,20 | 2,20 |
| RESPOND (RS) | Response Planning (RS.RP) | 3,00 | 5,00 | 4,00 |
| | Communications (RS.CO) | 3,00 | 4,00 | 2,40 |
| | Analysis (RS.AN) | 3,00 | 4,00 | 2,50 |
| | Mitigation (RS.MI) | 3,00 | 3,67 | 2,00 |
| | Improvements (RS.IM) | 3,00 | 4,00 | 2,00 |
| RECOVER (R | Recovery Planning (RC.RP) | 3,00 | 5,00 | 5,00 |
| | Improvements (RC.IM) | 3,00 | 4,00 | 3,50 |
| | Communications (RC.CO) | 3,00 | 4,00 | 2,67 |

**Figura 3.1 - Ilustração da simulação do registo de valores associados a lista de verificação**

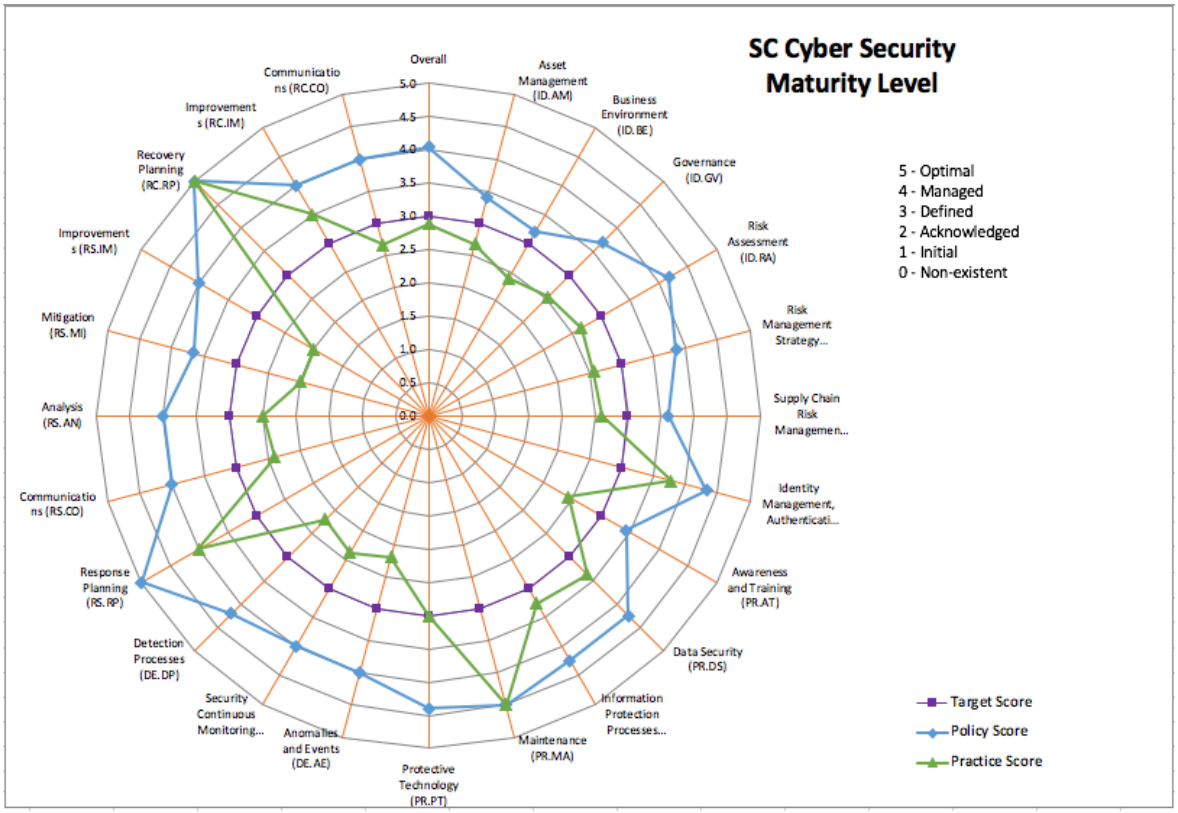


Figura 3.2 – Ilustração do gráfico geral de uma simulação da lista de verificação.

Neste contexto, e a título de exemplo, tendo como referência os valores recolhidos e ilustrados na Figura 3.1, o resultado apresentado na figura 3.2 permite analisar as Politicas / Praticas associadas ao nível de maturidade da Cibersegurança de uma infra estrutura tecnológica de uma SC. Com base nestes valores e neste tipo de ilustração os gestores, administradores e agentes de decisão da infraestrutura tecnológica das SC poderão ter uma perceção mais global e verificar em que dimensões intervir para mitigar (ou reduzir) os riscos de vulnerabilidade dos seus SI/TI na disponibilização dos serviços digitais aos cidadãos e ao eco sistema envolvente das SC.

Com base na metodologia de pesquisa mencionada acima, os resultados dos casos são apresentados no formulário, nomeadamente.

- Diagnóstico - identificar a pergunta de pesquisa. Neste caso de estudo, a pergunta foi "É possível que a cibersegurança seja um pilar necessário das cidades inteligentes?";
- Planeamento da Ação - Após o exame dos vários padrões e estruturas orientados para gerir e controlar o campo de TI, o fato é que a cibersegurança pode ser altamente considerada como um pilar das SCs baseados em infraestruturas tecnológicas e digitais;
- Ação - Neste caso de estudo e em particular para esta instituição, foi necessário prosseguir com a análise e especificação de ações de todas as necessidades e dificuldades de diagnóstico nos serviços de informações existentes para o Controle de Segurança e Cibersegurança do SI. Seguindo as diretrizes de cibersegurança e segurança, as diretrizes de *Checklist* e COBIT, foram definidas orientações para monitorizar e avaliar a segurança da infraestrutura da SC;
- Avaliação - Para avaliar o uso e implementação da abordagem metodológica, definiu-se um conjunto de indicadores, sendo um baseado nos indicadores das especificações NIST, ISO 27001 e COBIT e outro com base na pontuação dos tópicos descritos na tabela 2; e
- Aprendizagem obtida - o resultado obtido foi o seguinte: Melhorar a qualidade da assistência disponibilizada pelos serviços administrativos; controlar e gerir os SI/TI de forma mais eficiente, definindo processos e indicadores para fazê-lo; reduziu o tempo de execução das tarefas; ajudou a definir indicadores especialmente para avaliar o desempenho dos serviços no campo de TI; ser capaz de definir questionários para identificar, avaliar e gerir a infraestrutura de TI relacionada à Cibersegurança em um ecossistema de SC.

# 4. Conclusão

## 4.1. Conclusões

Nos últimos anos, muitos relatórios, documentos e muitos padrões, estruturas e diretrizes para as especificidades dos desafios de Cibersegurança e para uso no contexto de SCs foram publicados. Com base nos conceitos gerais de SCs, segurança e Cibersegurança, apresentamos uma revisão da literatura neste artigo, focando o trabalho em quatro estruturas de cibersegurança (Instituto Nacional de Padrões e Tecnologia, NIST) para a Estrutura de Cibersegurança de Práticas Regulatórias do Setor Financeiro da Cibersegurança, Instituto SANS - Controles críticos de segurança para defesa cibernética eficaz, padrão ISO 270xx e projeto de estrutura de Cibersegurança aberta OWASP e avaliação de riscos de Cibersegurança. Abordagens para identificar, analisar e avaliar vulnerabilidades de segurança como um método de avaliação de risco COBIT e OWASP. Metodologia de pesquisa-ação para a pergunta de pesquisa "A cibersegurança é um pilar necessário das cidades inteligentes?" Concluímos que a cibersegurança (desafios e medidas de prevenção) é um pilar crucial dos SCs.

Na seção 1.3 foram apresentados os objetivos deste trabalho, nos quais consideramos que todos foram conseguidos:

- Revisão da Literatura e estudo do estado da arte associado às SC, Segurança Informática e Cibersegurança – Foram analisados um largo conjunto de informação associada às SC, associado à cibersegurança e à relação entre ambos, as quais se apresentam na seção da bibliografia e das referências bibliográficas.
- Identificação e estudo de um conjunto de linhas orientadoras, normas e *frameworks* utilizadas a nível mundial para avaliar e mitigar a problemática associada à Segurança Informática e à Cibersegurança em especial quando aplicados às SC- Foram consideradas as informações e orientações das seguintes instituições, normas e *frameworks*: Control Objectives for Information and Related Technology (COBIT), Council on CyberSecurity (CCS) Top 20 Critical Security Controls, ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems, ISO/IEC 27001, Information technology - Security techniques - Information security management systems e as orientações gerais da ISO 27032 – Cybersecurity

guideline, OWASP Open Cyber Security Framework assim como as orientações da SANS Institute - Critical Security Controls for Effective Cyber Defense e do Financial Industry Regulatory Authority, no seu relatório de boas práticas a ter em conta em relação á cibersegurança.

- Definição de uma lista de verificação (*checklist*) do estado da relação SC com a Cibersegurança em cenários em que as SC assentam os seus serviços em SI/TI – A lista de verificação é apresentada na tabela 2.1 assim como as 185 questões das funções, domínios e subcategorias a contemplar na análise do estado de situação da segurança cibernética de uma SC.
- Aplicação da lista de verificação a um caso de estudo real – A lista foi aplicada em termos de simulação a uma SC de um município do norte de Portugal. Trata-se de uma primeira aproximação de análise que se pretende alargar o âmbito de teste e de aplicabilidade.
- Análise, discussão de resultados e divulgação das conclusões – Como resultado deste trabalho, além do conhecimento adquirido, o conhecimento transmitido aos gestores e administradores da infraestrutura tecnológica da SC, através de reuniões sobre a maturidade e questões associadas às SC e consequentemente à segurança cibernética. Estas reuniões funcionaram também como forma de divulgação da aprendizagem, sendo a publicação de um artigo numa conferência internacional indexada um dos principais resultados de divulgação.

Tendo como base a metodologia de investigação *Action Research*, os resultados das etapas foram as seguintes:

• Diagnostico — Identificou-se a questão de investigação. Neste caso a questão "É possível que a cibersegurança seja um pilar necessário nas cidades inteligentes/Smart Cities?";

• Planeamento da Ação — Depois de se analisar e estudar vários estudos, orientações, normas e *frameworks,* foi criada uma lista de verificação para analisar o estado da segurança cibernética de uma infraestrutura tecnológica de uma SC e identificadas 185 questões de análise;

• Tomada da Ação — Neste caso de estudo, foi simulada numa cidade "inteligente" do norte de Portugal;

• Avaliação — Para avaliar a lista de verificação foi utilizada uma abordagem metodológica de ponderação de pesos e pontuações, a qual é apresentada na secção 3.3.

• Aprendizagem Obtida —A aprendizagem obtida poderá ser considerada em várias vertentes pessoal, para as instituições em análise da segurança cibernética no sentido mitigar os riscos de vulnerabilidades, de melhorar a qualidade serviço, gerir de forma eficiente os SI/TI. Os dados de análise poderão ser obtidos através de questionários para identificar, avaliar, gerir e monitorizar o estado da infraestrutura tecnológica de uma SC face à cibersegurança e face ao seu "ecossistema".

## 4.2. Resultados

Como resultado direto deste trabalho apresenta-se:

- Uma lista de verificação sobre cibersegurança passível de ser testada numa infraestrutura tecnológica de uma SC para avaliar o seu estado de situação em relação à Cibersegurança.
- Como conjunto de linhas orientadoras associadas à segurança informática e à cibersegurança em particular passíveis de complementar a informação a ser analisada em cada item de análise na infraestrutura tecnológica das SC e considerando por um lado a ampla divulgação a nível mundial e por outro a elevada relevância das instituições associadas, como linhas orientadoras de suporte a cada item (ou subcategoria) da lista de verificação, consideramos relevante a consulta da seguinte informação:
  - NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (including updates as of January 15, 2014). http://dx.doi.org/10.6028/NIST.SP.800- 53r4.
  - Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
  - Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC): http://www.counciloncybersecurity.org
  - ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program:

http://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisplay.cfm&ProductID=10243

- ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels: http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=13420
- ISO/IEC 27001, Information technology - Security techniques -- Information security management systems -- Requirements: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534

Como resultado indireto deste trabalho, o estudo das características, particularidades, problemáticas, casos de estudo reais, linhas orientadoras, normas e *frameworks* associados às SC e à cibersegurança em particular na literatura escrita, online e em eventos tecnológicos mundiais em que participei, assim como na aplicabilidade de uma lista de verificação do estado da Cibersegurança numa SC, permitiu enriquecer os meus conhecimentos sobre estas temáticas, assim como o desafio de efetuar um primeiro teste de aplicabilidade real na análise do estado da cibersegurança numa SC.

## 4.3. Perspetivas Futuras

Embora os objetivos traçados fossem atingidos e o conhecimento adquirido enriquecedor em termos pessoais e profissionais, considero que, apesar da lista de verificação ser ampla e abrangente na análise dos pontos associados à cibersegurança nas SC, a mesma deverá ser testada noutras SC de modo a puder ser melhorada em termos de mais algum detalhe de análise, em particular face às particularidades da evolução tecnológica e dos vários tipos de serviços digitais associados, por exemplo à nova era de comunicação 5G com a interligação de novos equipamentos eletrónicos na infraestrutura tecnológica das SC. Por outro lado, no futuro, pretendemos explorar a recolha de dados da infraestrutura tecnológica das SC para potenciar o uso dos algoritmos e técnicas da Inteligência Artificial, por exemplo utilizando as redes neurais artificiais e sistemas de raciocínio baseado em casos, a fim de avaliar e prever padrões da Cibersegurança.

# Referências

## Bibliografia

Angelidou, M. (2016). Four European Smart City Strategies. International Journal of Social Science Studies Vol. 4, No. 4, ISSN 2324-8033 E-ISSN 2324-8041. DOI: 10.11114/ijsss.v4i4.1364

Armin, A., Junaibi, R., Aung, Z., Woon, W. e Omar, M. (2017). *Cybersecurity for Smart Cities: A Brief Review*. Lecture Notes in Computer Science. 10097. pp.22-30. DOI: 10.1007/978-3-319-50947-1_3

Avison, D., Lau, F., Myers, M. e Nielsen, P. (1999). Action Research. Commun. ACM, vol. 42 Issue 1, pp:94-97, https://doi.org/10.1145/291469.291479.

Ayoub, A., Zahi, B., Sabir, E. e Sadik, M. (2016). *A literature review on Smart Cities: Paradigms, opportunities and open problems*. International Conference on Wireless Networks and Mobile Communications (WINCOM), pp. 180-186. doi: 10.1109/WINCOM.2016.7777211

Bawany, N. e Shamsi, J. (2015). *Smart City Architecture: Vision and Challenges*. International Journal of Advanced Computer Science and Applications, 6(11), 246-255.

Bin Bishr, A. (2015). Smart Dubai: Introduction, Strategy and Progress Report. Paper presented at the ITU Forum on Smart Sustainable Cities, Abu Dhabi-UAE. Disponível em: https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2015/SSC/S1-DrAishaBinBishr.pdf (acedido em 30-07-2019).

Evans, M., Maglaras, L., Ying, H. e Helge, J. (2016). *Human Behaviour as an aspect of CyberSecurity Assurance*. In Security and Communication Networks. 9. https://doi.org/10.1002/sec.1657

Gaur, A., Scotney, B., Parr, G., e McClean, S. (2015). Smart City Architecture and its *Applications Based on IoT*. Procedia Computer Science, 52, 1089-1094. doi: https://doi.org/10.1016/j.procs.2015.05.122

Hazel S. e Taeihagh, A. (2018). *Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications*, Energies, Vol 11, p. 1062. http://dx.doi.org/10.3390/en11051062.

Hevner, A., March, S., Park, J., e Ram, S. (2004). Design Science in Information Systems Research. MIS Quarterly, 28(1), pp:75–105.

Ijaz, S., Shah, M., Khan, A. e Mansoor. A. (2016). *Smart Cities: A Survey on Security Concerns*. In International Journal of Advanced Computer Science and Applications. vol 7. DOI: 10.14569/IJACSA.2016.070277

Jansäter G. e Olsson, J. (2018). Cyber Security in Smart Cities-Not a primary concern. Master thesis, Lund Uiversity - Department of Informatics. Disponível em: http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8950557&fileOId=8950904

Khan, M., Woo, M., Nam, K. e Chathoth, P. (2017). Smart City and Smart Tourism: A Case of Dubai. Sustainability Journal. DOI: 10.3390/su9122279

Khatoun, R. e Zeadally, S. (2017). *Cybersecurity and Privacy Solutions in Smart Cities*. IEEE Communications Magazine IEEE Commun. Mag. Communications Magazine, IEEE. 55(3):51-59.

Kilani, M. e Kobziev, V. (2016). *An Overview of Research Methodology in Information System (IS)*. Open Access Library, 3, pp.1-9.

Lévy-Bencheton, C. e Darra, E. (2015). *Cyber security for Smart Cities: An architecture model for public transport*. Greece. Disponível em https://www.enisa.europa.eu/publications/smart-cities-architecture-model/at_download/fullReport (acedido em 30-07-2019).

Li, Z. e Liao, Q. (2018). *Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets*, Government Information Quarterly. Vol. 35 Issue 1, p151-160. https://doi.org/10.1016/j.giq.2017.10.006

Lim, H., e Taeihagh, A. (2018). *Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications*. Energies, vol 11, no 5:1062.

Mijac, M., Androcec D. e Picek, R. (2017). *Smart city services driven by IoT: a systematic review*. In Journal of Economic and Social Development (Varaždin), vol 4, pp.40-50.

Monzon, A. (2015). *Smart cities concept and challenges: Bases for the assessment of smart city projects*. In Smart Cities and Green ICT Systems, 2015 International Conference on, pp. 1–11.

Olesen, K.e Myers, D. (1999). *Trying To Improve Communication And Collaboration With Information Technology*. Information Technology & People, 12, (4), pp: 317-332. https://doi.org/10.1108/09593849910301621

Peffers, K., Tuunanen, T., Rothenberger, M. A., e Chatterjee, S. (2007). *A Design Science Research Methodology for Information Systems Research*. Journal of Management Information Systems, 24(3), pp:45–77.

Ribeiro, J., Alves, V., Vicente, H., e Neves, J. (2019). *Planning, Managing and Monitoring Technological Security Infrastructures*. Lecture Notes in Electrical, vol. 505, Springer Verlag Eds. https://doi.org/10.1007/978-3-319-91334-6_2

Waedt, K., Ciriello, A., Parekh, M. e Bajramovic, E. (2016). *Automatic assets identification for smart cities: Prerequisites for cybersecurity risk assessments*. IEEE International Smart Cities Conference (ISC2) Smart Cities Conference (ISC2), pp:1-6.

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., e Shen, X. (2017). *Security and Privacy in Smart City Applications: Challenges and Solutions*. IEEE Communications Magazine. 55. Pp.122-129, 2017.

Zhiyi, L. e Shahidehpour, M. (2017). *Special Issue: Contemporary Strategies for Microgrid Operation & Control: Deployment of cybersecurity for managing traffic efficiency and safety in smart cities*. Special Issue: Contemporary Strategies for Microgrid Operation & Control, The Electricity Journal, 30(4):52-61.

## Referências Bibliográficas

[1] ESPON - European Grouping on Territorial Cooperation (2017). Policy Brief: The territorial and urban dimensions of the digital transition of public services. Disponível em: https://www.espon.eu/digital-transition

[2] Outlier Ventures (2016). Convergence in Smart Cities Building the Digital Infrastructure for the Fourth Industrial Revolution. Disponível em:

https://www.smartdubai.ae/docs/default-source/default-document library/convergenceinsmartcities_en.pdf

[3] KMG (2015). Dubai - a new paradigm for smart cities. Disponível em: https://assets.kpmg/content/dam/kpmg/pdf/2016/04/Dubai-a-new-paradigm-for-smart-cities-uae.pdf

[4]. Greater London Authority (2018). Smarter London Together The Mayor's roadmap to transform London into the smartest city in the world. Disponível em: https://www.london.gov.uk/sites/default/files/smarter_london_together_v1.66_-_published.pdf

[5] Josep-Ramon Ferrer (2017). *Barcelona's Smart City vision: an opportunity for transformation. Journal of Field Actions Science Reports*. Special Issue 16, p.70-75. Disponível em: https://journals.openedition.org/factsreports/4367

[6] Ed Holder (2019). City of London – Canadá – Strategic Plan for 2019-2023. Disponível em: https://www.london.ca/city-hall/Civic-Administration/City-Management/Documents/StrategicPlan_2019.pdf

[7] Häupl, M e Vassilakou , M. (2016). Smart City Wien. Disponível em: https://smartcity.wien.gv.at/site/files/2019/07/Smart-City-Wien-Framework-Strategy_Overview_2014-resolution.pdf

[8] Newcastle City Council (2017). 2017-2021 – Smart City NewCastle Stratetegic Plan. Disponível em: https://www.newcastle.nsw.gov.au/getattachment/Business/Smart-City/smart-city/2752_Smart-City-Strategy-FINAL-WEB-indexed.pdf.aspx?lang=en-AU

[9] Iveson D., (2017). Edmonton Smart City Strategic Plan. Disponível em: https://www.edmonton.ca/city_government/documents/PDF/Smart_City_Strategy.pdf

[10] Crouse, N. (2016). City of St. Albert (USA) Smart City Master Plan. Disponível em: https://stalbert.ca/uploads/PDF-forms/Smart_City_Master_Plan_-_Summary_-_web.pdf

[11] ITU International Telecommunication Union - Global Cybersecurity Index 2017. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

[12] KPMG (2019). Cybersecurity in smart cities. Disponível em: https://assets.kpmg/content/dam/kpmg/in/pdf/2019/02/Cybersecurity-in-smart-cities.PDF

[13] SANS Institute, Evaluating Cyber Risk in Engineering Environments: A Proposed Framework and Methodology. Rebekah Mohr. Disponível em https://www.sans.org/reading-room/whitepapers/ICS/paper/37017

[14] PWC Consulting (2018), Creating cyber secure smart cities. Disponível em: https://www.pwc.in/assets/pdfs/publications/2018/creating-cyber-secure-smart-cities.pdf

[15] European Commission: Assess city's digital maturity Tool: https://www.digitallytransformyourregion.eu/assess-your-citys-digital-maturity,

[16] European SmartCities Benchmarkink Assessment: http://www.smart-cities.eu.

[17] European Union Agency for Network and Information Security (ENISA). Disponível em: https://www.smesec.eu

[18] ISO 27001 - International Organization for Standardization - Information security management systems. Disponível em: https://www.iso.org/isoiec-27001-information-security.html

[19] COBIT: Information Systems Audit and Control Association, Control Objectives for Information and Related Technology, 5th Edition, IT Governance Institute, (2019). Disponível em: https://www.isaca.org

[20] OGC: Official Introduction to the ITIL Service Lifecycle, Stationery Office, Office of Government Commerce (2019). Disponível em: https://www.itgovernance.co.uk

[21] Financial Industry Regulatory Authority, Inc. Financial Industry Regulatory Practices (2018). Disponível em: https://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf

[22] National Institute of Standards and Technology (NIST) Cybersecurity Framework (2014). Disponível em: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[23] SANS Institute - Critical Security Controls for Effective Cyber Defense. Disponível em: https://www.sans.org/critical-security-controls.

[24] ISO 27032 - Information technology — Security techniques — Guidelines for cybersecurity (2019), Disponível em: https://www.iso.org/standard/44375.html

[25] Open Cyber Security Framework Project, OWASP Open Cyber Security Framework Project. Disponível em:

https://www.owasp.org/index.php/OWASP_Open_Cyber_Security_Framework_Project.

[26] Ernest & Yong (2018). Cybersecurity and the Internet of Things. Disponível em: https://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/%24FILE/EY-cybersecurity-and-the-internet-of-things.pdf

[27] NITI Aayog (Hindi for Policy Commission) - (2018). Indian Cybersecurity framework Case Study. disponível em: https://www.niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf

# Anexos

## A . Publicações

| | |
|---|---|
| Título | CYBERSECURITY - A PILLAR FOR SMART CITIES |
| | Vaz P., Ribeiro, J., Neves, J., Frazão, F., "CYBERSECURITY - A PILLAR FOR SMART CITIES". In Procs of the 73rd Research World International Conference, Tokyo, Japan, 7th-8th September, 2019, ISBN 978-93-89469-07-3. |
| Conferência | Proceedings of the 73rd Research World International Conference, Tokyo, Japan, 7th-8th September, 2019, ISBN 978-93-89469-07-3. |
| Indexação | SCOPUS, Google Scholar |

# B . Programa dos Eventos Tecnológicos