risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 20/06/2022
Aceitação/Acceptance: 30/10/2022

Um Inquérito para Verificação da Cibersegurança nas Organizações Públicas Municipais em Portugal

Teófilo T Branco Jr[1], Isabel Celeste da Fonseca[1]

teofilotb@hotmail.com; isabel.uminho@gmail.com

[1] Universidade do Minho, Escola de Direito, Campus de Gualtar, CP 4710-057, Braga, Portugal

DOI: 10.17013/risti.48.41–58

Resumo: A estrutura tecnológica das organizações expandiu-se e o número de utilizadores aumentou consideravelmente com o avanço na digitalização dos serviços. Por conseguinte, é necessário implementar medidas de segurança para preservar as ameaças e riscos relacionados com a segurança dos dados. Para isso, foi desenvolvido um inquérito com o objetivo de fornecer um panorama da situação em que se encontra a segurança cibernética nas organizações contendo os principais pontos de controlo a serem observados. Este trabalho foi realizado com base na revisão da literatura e entrevistas com especialistas. O objetivo deste inquérito é possibilitar a verificação dos quesitos relacionados com a cibersegurança nos orgãos da administração de governos municipais para que estes se previnam melhor dos ciber ataques.

Palavras-chave: Cibersegurança; Governo Eletrónico; Lei de Segurança Cibernética; Privacidade de Dados; Segurança da Informação.

A Survey to Verify Cybersecurity in Municipal Public Organizations in Portugal

Abstract: The technological structure of organizations has expanded, and the number of users has increased considerably with the advance in the digitalization of services. Therefore, it is necessary to implement security measures to preserve the threats and risks related to data security. To this end, a survey was developed to provide an overview of the cybersecurity status quo in organizations containing the main control points to be observed. This work was carried out based on a literature review and expert interviews. The objective of this survey is to enable the verification of cybersecurity-related issues in the administrative organs of municipal governments so that they can better prevent cyber attacks.

Keywords: Cybersecurity; Cybersecurity Law; Data Privacy; e-Government; Security Information.

1. Introdução

Um estudo da Capgemini, juntamente com o IDC e o Instituto Politécnico de Milão, sobre o nível dos serviços de governo eletrônico na Europa, foi publicado no eGovernment

Benchmark 2021 (European Commission & DG CONNECT, 2021) . Ele revelou que a situação pandêmica causada pela COVID-19 pressiona os governos europeus a mudar a forma como os serviços públicos de governo são prestados.

Muito serviços anteriormente prestados presencialmente tiveram que migrar para a modalidade "on-line". O estudo concluiu que mais de oito em cada dez dos serviços públicos avaliados (81%) estão agora disponíveis on-line. O estudo também revela que os governos de toda a Europa fizeram progressos consideráveis na digitalização da prestação de serviços públicos, demonstrando com sucesso sua capacidade de fornecer serviços online adaptados à crise global que surgiu na esteira da pandemia.

Por outro lado, houve também um forte aumento dos casos de ataques cibernéticos em 2019 (Lallie et al., 2021). Os ciber ataques também visaram infraestruturas nacionais críticas, tais como saúde e serviços. Em resposta, em 8 de abril de 2020, o National Cyber Security Center (NCSC) do Reino Unido e a Agência de Segurança Cibernética e Infraestrutura (CISA) do Departamento de Segurança Interna (DHS) dos Estados Unidos publicaram uma assessoria conjunta sobre como os grupos ciber-criminosos e as ameaças persistentes avançadas (APT) estavam explorando a pandemia da COVID-19. Esta assessoria discutiu plataformas de phishing, malware e comunicações (por exemplo, Zoom, Microsoft Teams, e outros). Os ataques foram relatados por governos, organizações de segurança, e equipes de incidentes (Lallie et al., 2021).

Há uma diversidade de alvos de ameaças cibernéticas, desde instituições públicas até cidadãos comuns. Entretanto, os principais alvos dos ataques estão inter-relacionados. Por exemplo, as ameaças cibernéticas em instituições governamentais são geralmente centradas em seus sistemas de informação. As implicações podem ser catastróficas porque, entre estas instituições, podem existir hospitais, escolas e até mesmo usinas de energia nuclear (Carvalho et al., 2020).

De acordo com (Lallie et al., 2021), como o crime tradicional, o crime cibernético é frequentemente descrito pelo triângulo do crime envolvendo três fatores: uma vítima, motivo e oportunidade. A vítima é o alvo. A razão é o aspeto que leva o criminoso a cometer o ataque e a oportunidade é a vulnerabilidade que existe para que o crime seja alcançado. Embora hoje os ataques se tenham tornado mais sofisticados e direcionados a vítimas específicas, também prevalecem os ataques oportunistas não direcionados. Um ataque oportunista explora as vítimas, geralmente na engenharia social, onde os ganchos criam estas vulnerabilidades. Assim, podemos definir a palavra "gancho" como qualquer mecanismo usado para enganar uma vítima a cair na armadilha de um ataque. Estes ganchos aproveitam a distração, a falta de critérios, controles e outros fatores administrativos e humanos.

Embora também ocorram ataques envolvendo vulnerabilidades técnicas em software e hardware e não apenas em aspetos humanos, os atacantes também tentam aproveitar todas as oportunidades. Consequentemente, várias diretrizes e recomendações também foram publicadas para proteger contra ataques ao exemplo de entidades como ENISA, FTC, NCSC, e NIST (Lallie et al., 2021).

Neste artigo, são apresentados os estudos que orientaram o desenvolvimento deste instrumento e as expectativas de sua aplicação nas organizações públicas municipais.

1.1. Objetivos da investigação

O objetivo deste estudo é fornecer informações sobre as condições atuais e desejadas para preparar as condições necessárias para a transição para cidades inteligentes. A partir da compreensão amadurecida da Governança Eletrônica, será possível elaborar um plano global para a transição digital dos governos locais (Fonseca, 2020).

Neste sentido, a identificação de pontos de controle relacionados aos princípios de cibersegurança é um indicador importante. Através deste modelo de verificação, é possível identificar riscos, aumentar a conscientização das administrações locais, propor recomendações e ajudar na concepção de projetos para corrigir as lacunas existentes. Além disso, as análises e opiniões dos especialistas envolvidos podem justificar a obtenção dos recursos necessários para implementar as medidas necessárias.

1.2. Metodologia

Esta investigação explora a perceção do gerenciamento de TI sobre a situação atual de cibersegurança na infraestrutura de conectividade local e no gerenciamento de recursos de TI. Esta perceção proporciona uma compreensão dos princípios e recomendações para preservar a segurança dos sistemas de informação. Também destaca a necessidade de melhorar os procedimentos, técnicas e a aquisição de tecnologias para monitorar e controlar a segurança cibernética pela gerência local nas organizações.

Foram empregadas técnicas como revisão de literatura, entrevistas com administradores de TI e especialistas. Como resultado, foi desenvolvido um modelo de verificação para identificar lacunas relacionadas aos princípios e boas práticas relativas à cibersegurança.

Para o atingimento dos objetivos deste estudo, foram formuladas as seguintes questões de pesquisa:

Q1: Quais são as principais recomendações relativa a cibersegurança da comunidade científica, entidades governamentais e não governamentais?

Q2: Como verificar se a cibersegurança nas organizações públicas está em conformidades com as recomendações e legislação pertinentes?

2. Referencial Teórico

A evolução tecnológica alcançada nos últimos tempos proporciona condições para a criação de soluções envolvendo conceitos inovadores e o potencial a ser aplicado no setor governamental, promovendo a interface entre o cidadão e a estrutura do governo local através da digitalização dos serviços públicos. Além de terem a capacidade de proporcionar melhor eficiência operacional, estas soluções podem oferecer economia de recursos através da otimização de processos. Entretanto, no contexto dos recursos tecnológicos, as ameaças de ataque a este cenário digital também estão melhorando através de formas cada vez mais evoluídas de crime no mundo cibernético. Portanto, os riscos de crimes cibernéticos devem ser compreendidos e mitigados.

A solução proposta neste estudo explora conceitos e tecnologias como governo eletrônico e segurança cibernética para melhorar e otimizar a gestão administrativa de governos locais e entidades privadas. Para entender melhor o potencial proporcionado por estes

conceitos tecnológicos, sociais e inovadores, procuramos identificar alguns trabalhos que abordam estes conceitos. Este referencial tem o objetivo de esclarecer detalhes essenciais na aplicação destas tecnologias sem contexto social e as experiências de lições descritas em artigos acadêmicos e recomendações de entidades especializadas. A Tabela 1 relaciona o referencial teórico utilizado neste estudo.

Tema	Referência
Estudo sobre alavancagem de crimes cibernéticos com dispositivos interconectados	(Reyes-Menendez et al., 2020)
Revisão da Literatura sobre as perspetivas de risco consideradas na implementação do conceito de cidades inteligentes.	(Sharif & Pokharel, 2022)
Revisão da Literatura sobre os riscos em atividades típicas on-line	(Wirtz & Weyerer, 2016)
Objetivos estratégicos para o alinhamento com a Comissão Europeia de Segurança Cibernética	(Carvalho et al., 2020)
Análise do Regime de Segurança do Ciberespaço em Portugal (Lei nº 46/2018, de 13 de agosto)	(Osório De Barros, 2018)
ISO/IEC 27002:2022 é um documento que fornece um conjunto de referência de controles genéricos de segurança da informação sobre segurança da informação, segurança cibernética e proteção da privacidade	(International Organization for Standardization - ISO, n.d.)
Documento "National Cyber Security Strategies (NCSS)", onde são estabelecidos os princípios estratégicos, diretrizes, objetivos e medidas específicas para mitigar o risco associado à cibersegurança.	(E. U. A. for C. ENISA, n.d.)

Tabela 1 – Referencial Teórico

2.1. Revisão da Literatura

(Reyes-Menendez et al., 2020) fazem uma revisão da literatura sobre o crescimento exponencial do número de cibercrimes no ambiente digital de negócios, com o objetivo de identificar o risco de invasão nos sistemas e dispositivos de Internet das Coisas (IoT). Os autores propõem soluções que possam evitar ciber ataques em reforço a segurança cibernética neste ambiente.

Um estudo de revisão de literatura realizado por (Sharif & Pokharel, 2022) aborda as perspetivas de risco consideradas na implementação do conceito de cidades inteligentes. Os autores sustentam que se tais riscos não forem compreendidos e tratados, eles podem criar problemas em termos de privacidade e segurança e, portanto, afetar o funcionamento das cidades inteligentes. Neste estudo, os riscos das cidades inteligentes são relacionados à tecnologia, à organização e ao meio ambiente externo.

Os riscos técnicos estão relacionados à tecnologia e sua implementação, tais como os riscos associados à IdC, BigData e IA como os mais importantes.

O estudo conduzido mostra que os riscos não técnicos têm um efeito percetível na implementação e operação de cidades inteligentes. Eles destacam questões relacionadas

à governança e diferenças legais e organizacionais entre os setores público e privado em cidades inteligentes. Os riscos não técnicos são riscos socioeconômicos, de governança e legais e estratégicos (Sharif & Pokharel, 2022). Os autores sustentam que os riscos socioeconômicos incluem a mentalidade tradicional das partes interessadas e dos tomadores de decisão. Implementar o conceito de cidades inteligentes significa gerenciar projetos multidisciplinares que requerem um orçamento considerável, pessoal treinado e exposição tecnológica de cidadãos, tomadores de decisão e profissionais.

Outra preocupação é gerenciar questões legais relacionadas à privacidade dos dados e riscos de proteção de dados dentro de projetos de "cidades inteligentes".

De acordo com (Wirtz & Weyerer, 2016), as fontes potenciais de risco incluem atividades típicas on-line, tais como navegação na web, comunicação por e-mail, programas de mensagens, acesso a redes sociais e uso de redes sem fio. Em adição, elas também têm mais atividades relacionadas à gestão, tais como terceirização de atividades administrativas para fornecedores privados. Portanto, identificar vulnerabilidades e ameaças e suas potenciais consequências como parte da análise de risco é essencial para implementar medidas de segurança apropriadas.

As preocupações de segurança dos funcionários de TI da administração pública e dos cidadãos representam outro fator de risco que caracteriza o estado de segurança cibernética no setor público.

Também, de acordo com (Wirtz & Weyerer, 2016), outro fator de risco refere-se à falta de consciência de risco da autoridade superior. Embora a conscientização da segurança deva aumentar em todos os níveis administrativos, pesquisas têm mostrado que a falta de entendimento sobre questões relacionadas à cibersegurança entre os funcionários, especialmente no nível executivo, desempenha um papel crucial na cibersegurança no setor público.

Os autores afirmam que 80% dos acidentes de segurança da informação são resultantes de causas internas. As medidas de proteção cobrem um amplo espectro, desde medidas mais tradicionais, como controles de acesso físico ou treinamento de pessoal, até medidas mais modernas e tecnológicas, como firewall, software antivírus e tecnologias de criptografia. Caso tais medidas de proteção não consigam evitar um ataque cibernético, entra em jogo o gerenciamento de emergência, que é outro tipo crítico de recurso. O gerenciamento de emergências geralmente envolve o desenvolvimento e implementação de planos de ação para reduzir a vulnerabilidade a ameaças e enfrentar o impacto de desastres. Outro fator de risco se refere à experiência profissional e ao conhecimento especializado do pessoal.

Finalmente, o apoio de recursos pelas autoridades sênior tem como um fator de segurança cibernética. O apoio da alta administração está entre os aspetos mais frequentemente mencionados da implementação bem sucedida do sistema informático. No caso da administração pública, a aprovação da autoridade superior é essencial, já que esta última é geralmente responsável pelo fornecimento de fundos e outros recursos necessários para conduzir os projetos e medidas necessárias.

2.2. Objetivos estratégicos para o alinhamento com a Comissão Europeia de Segurança Cibernética

A União Europeia tem uma estratégia para promover a segurança de redes e sistemas de informação em seus estados membros. O principal objetivo é aumentar a capacidade dos governos, cidadãos e instituições para lidar com ciber ataques. A estratégia inclui a definição de procedimentos a serem adotados pelos governos na prevenção e resposta aos ciber ataques, e a cooperação e colaboração internacional entre os estados para combater o crime cibernético (Carvalho et al., 2020).

Na estratégia europeia de segurança de redes e informações, a Comissão Europeia procurou criar legislação para criminalizar tais crimes, aumentar a capacidade de segurança cibernética, promover o intercâmbio de informações entre países e assim estabelecer uma política internacional coerente de segurança cibernética para a União Europeia. A estratégia de segurança cibernética da União Europeia sugere que seus membros devem definir alguns requisitos mínimos padrão. Cada membro deve ter uma rede nacional competente e uma autoridade de segurança da informação, uma equipe de resposta a emergências (CERT) e uma estratégia nacional e um plano de cooperação entre os estados membros (Carvalho et al., 2020).

Outro passo crítico foi a adoção do Regulamento Geral de Proteção de Dados (GDPR), que foi aprovado em 15 de abril de 2016 e entrou em vigor em 25 de maio de 2018 (European Parliament and Council of the European Union, 2016) . A GDPR é uma regulamentação legal europeia sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos da União Europeia e do Espaço Econômico Europeu (EEE). Seu objetivo é dar aos cidadãos e residentes meios de controlar os dados pessoais. Ela também visa unificar a estrutura reguladora sobre privacidade e proteção de dados pessoais e regular a exportação de dados pessoais para fora da UE e da AEE. A GDPR contém cláusulas e exigências relativas à forma como as informações pessoais são processadas na União Europeia. Ela se aplica a todas as empresas que operam na AEE, independentemente de seu país de origem. Entre outras premissas, ela regulamenta isso: (a) Os dados devem ser armazenados usando pseudonímia ou anonimização completa, com a mais alta privacidade por padrão, de modo que os dados não possam ser disponibilizados sem consentimento explícito e não possam ser usados para identificar alguém sem informações adicionais armazenadas separadamente; (b) o responsável pelo tratamento deve indicar qualquer coleta de dados, indicar qual estrutura legal permite tal coleta, a finalidade do processamento de dados, por quanto tempo os dados serão armazenados e se tais dados serão compartilhados com terceiros fora da União; (c) as autoridades públicas e empresas que se concentram no processamento regular ou sistemático de dados pessoais devem ter um responsável pela proteção de dados (DPO), que é responsável por garantir que o processamento esteja em conformidade com a GDPR (Carvalho et al., 2020).

Com relação à resiliência aos ataques cibernéticos, a UE precisa de estruturas mais robustas e eficazes para garantir maior resiliência cibernética, promover a segurança cibernética e responder melhor aos ataques cibernéticos dirigidos aos Estados membros e às próprias instituições, agências e órgãos da UE. Ela também precisa de forte segurança cibernética para seu Mercado Único, avanços significativos nas capacidades tecnológicas dos membros e uma compreensão mais ampla do papel de todos no

combate às ameaças cibernéticas. Em resposta, a Comunicação Conjunta sugere novas iniciativas em três áreas-chave: a) fortalecer a resistência aos ataques cibernéticos e melhorar a capacidade de segurança cibernética da UE; b) criar uma resposta efetiva de justiça criminal; c) aumentar a estabilidade global através da cooperação (Carvalho et al., 2020). Complementarmente, a Agência de Segurança de Redes e Informações (ENISA) (E. U. A. F. C. ENISA, n.d.) foi criada para ajudar os Estados membros a lidar com os ciber ataques. O papel da ENISA é estabelecer um nível primário de segurança de rede e de dados na União Europeia, alertar os cidadãos sobre os riscos e promover uma cultura de segurança na Internet para os cidadãos da UE, consumidores, empresas e autoridades públicas.

2.3. A Lei de Cibersegurança em Portugal

Em Portugal, o Parlamento aprovou o regime de segurança do Ciberespaço (Lei nº 46/2018, de 13 de agosto (Assembleia da República, 2018)), transpondo a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, sobre medidas para garantir um alto nível de segurança de redes e informações em toda a União Europeia (Osório De Barros, 2018).

A Lei (Assembleia da República, 2018) aprovada pelo Parlamento Europeu prevê:

1. A definição de uma "Estratégia Nacional de Segurança do Ciberespaço";
2. A estrutura nacional de segurança do ciberespaço, incluindo a criação do "Conselho Superior de Segurança do Ciberespaço";
3. Identificar o ponto de contato nacional para cooperação internacional (Centro Nacional de Segurança Cibernética);
4. A definição dos requisitos de segurança em redes e sistemas de informação;
5. A aprovação das obrigações de comunicação de incidentes ao Centro Nacional de Segurança Cibernética;
6. A definição do regime de delitos aplica-se à violação da lei.

O Centro Nacional de Segurança Cibernética é a Autoridade Nacional de Segurança Cibernética, e a equipe nacional de resposta a incidentes de segurança cibernética (CSIRT) está subordinada a ela (Osório De Barros, 2018).

A Lei 46/2018 (Assembleia da República, 2018) estabelece regras para a Administração Pública (nomeadamente como operador de serviços essenciais), operadores de infraestrutura crítica, operadores de serviços essenciais, provedores de serviços digitais e qualquer entidade que utilize redes e sistemas de informação. Não obstante, a Lei se refere à definição de requisitos de segurança (artigos 14, 16 e 18) e requisitos de notificação de incidentes (artigos 15, 17 e 19) em sua legislação (artigo 31). Além disso, dado o nível de exigência e relevância do Regulamento Geral de Proteção de Dados (Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016), a Lei mencionada acima declara explicitamente que "não prejudica o cumprimento da legislação aplicável sobre proteção de dados pessoais".

2.4. Standard ISO/IEC 27002:2022

ISO/IEC 27002:2022 (International Organization for Standardization - ISO, n.d.) é um documento que fornece um conjunto de referência de controles genéricos de segurança

da informação sobre segurança da informação, segurança cibernética e proteção da privacidade. Controles de segurança da informação. Este documento é projetado para organizações de todos os tipos e tamanhos, Organizações de todos os tipos e tamanhos (incluindo o setor público e privado, comercial e sem fins lucrativos). Ele deve ser usado como referência para determinar e implementar controles para lidar com riscos de segurança da informação em um sistema de gerenciamento de segurança da informação (ISMS) baseado na ISO/IEC 27001.

2.5. National Cyber Security Strategies (NCSS)

A ENISA (E. U. A. for C. ENISA, n.d.) publicou um documento intitulado "National Cyber Security Strategies (NCSS)", que são os principais documentos dos Estados-Membros da UE para estabelecer princípios estratégicos, diretrizes e objetivos e, em alguns casos, medidas específicas para mitigar o risco associado à cibersegurança.

Para fortalecer a infraestrutura crítica contra várias ameaças e manter a confiança dos cidadãos da UE, a Comissão Europeia propôs a Diretiva de Segurança de Redes e Informações (Diretiva NIS) em 2013. Em dezembro de 2015, o Parlamento Europeu e o Conselho chegaram a um acordo sobre a proposta da Comissão. O Parlamento Europeu adotou a diretiva final em julho de 2016, e ela entrou em vigor em agosto de 2016.

O Centro Nacional de Segurança Cibernética (NCSC) publicou em 2021 um guia (NCSC, 2021) contendo orientações para ajudar as autoridades locais a compreender as considerações de segurança necessárias para projetar, construir e gerenciar cidades inteligentes. Além disso, o manual recomenda um conjunto de princípios de segurança cibernética que podem ajudar a proteger um lugar conectado e sua infraestrutura subjacente para ser mais resistente a ataques cibernéticos e mais fácil de gerenciar. De acordo com o NCSC, o guia é particularmente relevante para administradores de segurança da informação, CISOs, arquitetos e engenheiros de segurança cibernética e todo o pessoal que irá gerenciar as operações diárias da infraestrutura da rede cibernética.

3. Entrevistas com Administradores de TI e especialistas

Após a revisão da literatura, foi elaborado um documento contendo os principais pontos para verificação da segurança cibernética a partir das recomendações ali contidas. Estes pontos foram elencados em tópicos a partir da estrutura do guia (NCSC, 2021) para sua organização.

A seguir, foram realizadas entrevistas individuais com cinco administradores de TI de uma organização pública municipal para opinarem sobre os pontos que ofereciam alto risco e impacto em ataques cibernéticos. Um jurista especialista em legislação sobre o tema de proteção a privacidade de dados foi também entrevistado para opinar quais seriam os pontos a serem verificados para o atendimento à legislação sobre a cibersegurança em Portugal. A seleção dos profissionais se deu pela sua atuação, função, tempo de experiência no cargo e sua formação/especialização. A Tabela 2 elenca o perfil dos profissionais de TI e especialistas envolvidos nas entrevistas.

Setor de Atuação	Função	Tempo de Experiência	Formação Académica/ Especialização
Administração Pública Municipal	Gestor de Núcleo de TI	15 anos	Doutor/Analista de Sistemas
Administração Pública Municipal	Gestor de Núcleo de TI	10 anos	Mestre/Analista de Sistemas
Administração Pública Municipal	Gestor de Núcleo de TI	5 anos	Especialista/Analista de Sistemas
Administração Pública Municipal	Gerente de Segurança de TI	4 anos	Graduado/Técnico de TI
Administração Pública Municipal	Gerente de Segurança de TI	4 anos	Graduado/Técnico de TI
Universidade Pública	Investigador	2 anos	Mestre / Bacharel em Direito

Tabela 2 – Administradores de TI e especialistas entrevistados

A seleção dos pontos de verificação se deu através do consenso e de algum novo ponto considerado relevante por algum dos entrevistados. Na ocorrência de algum novo ponto sugerido, o mesmo era submetido aos outros para avaliação. A contribuição do jurista se deu ao final para verificação de possível acréscimo de algum ponto da legislação que necessite ser observado e que porventura ainda não estivesse elencado.

4. O Inquérito

O objeto resultante deste estudo e das entrevistas culminou em um inquérito que tem por objetivo a verificação de pontos de verificação críticos para a cibersegurança em órgãos públicos municipais.

O questionário contém dez seções e 133 questões e pode ser consultado no anexo a este trabalho.

5. Discussões e Conclusões

A equipe do projeto, após avaliação geral do instrumento, considerou que o instrumento elaborado permite avaliar o estágio da cibersegurança nas organizações públicas municipais. O instrumento foi considerado como sendo de fácil entendimento pelos administradores de TI e por todos os entrevistados. pode revelar a necessidade de implementar políticas locais de segurança e a necessidade de treinamento e educação corporativa. Ele pode propiciar às organizações realizarem análises a fim de aferir sua maturidade em relação à segurança cibernética.

Entretanto, apesar do instrumento permitir que sejam avaliadas as atividades de monitoramento e controle de cibersegurança no dia a dia das organizações, a tomada de decisões dos gestores dos órgãos e dos gerentes da unidades administrativas desempenham papel essencial para a gestão da cibersegurança, a partir da colaboração com a equipe de TI e do incentivo às boas práticas no ambiente de trabalho.

Campanhas educacionais também devem ser implementadas para sensibilizar os utilizadores a desenvolver hábitos voltados para a segurança da informação.

Embora o inquérito tenha sido desenvolvido para aplicação em organizações da administração pública municipal em Portugal, a equipe considera que o instrumento possa se adequar para realizar verificações da cibersegurança em outras organizações em geral. Neste sentido, as questões poderão ser adaptadas de acordo com as características da organização, inserindo questões mais detalhadas ou até mesmo suprimir as que não se aplicam à sua realidade operacional.

6. Limitações do estudo

Os aspetos de segurança relacionados à proteção de equipamentos e dispositivos físicos, notadamente quando se trata do uso da Internet sem fio, não foram objeto deste estudo, por serem de responsabilidade dos fabricantes e fornecedores de hardware. Os relacionados à computação em nuvem e Inteligência Artificial também não fizeram parte deste estudo por serem estas questões em um nível técnico mais aprofundado.

7. Estudos Futuros

Este estudo é parte de uma iniciativa do projeto "Smart Cities and Law, E-Governance and Rights: Contributing to the definition and implementation of a Global Strategy for Smart Cities.", com a referência NORTE-01-0145-FEDER-000063, na Escola de Direito da Universidade do Minho, Portugal.

Em colaboração com a administração local dos municípios, este projeto desenvolve vários estudos em parceria com centros de excelência tecnológica e a comunidade científica acadêmica.

O inquérito desenvolvido será aplicado nos municípios abrangidos pelo projeto para verificar as práticas atuais de cibersegurança.

A partir das análises advindas destas verificações, será possível sugerir orientações, medidas corretivas necessárias e sugestões de projetos para melhorar a cibersegurança local.

Referências

Assembleia da República. (2018). Lei n.º 46/2018 Regime jurídico da segurança do ciberespaço. *Diário Da República n.º 155/2018, Série I de 2018-08-13*, 4031–4037. https://dre.pt/home/-/dre/116029384/details/maximized

Carvalho, J. V., Carvalho, S. & Rocha, Á. (2020). European strategy and legislation for cybersecurity: implications for Portugal. *Cluster Computing*, *23*(3), 1845–1854. https://doi.org/10.1007/s10586-020-03052-y

ENISA, E. U. A. F. C. (n.d.). *ENISA*. https://www.enisa.europa.eu/

ENISA, E. U. A. for C. (n.d.). *National Cybersecurity Strategies Guidelines & tools*. Retrieved May 14, 2022, from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools

European Commission & DG CONNECT. (2021). eGovernment Benchmark 2021: Entering a New Digital Government Era: Insight Report. In *Luxembourg, Publications Office of the European Union, 2021*. https://data.europa.eu/doi/10.2759/55088

European Parliament and Council of the European Union. (2016). General Data Protection Regulation - GDPR. *Official Journal of the European Union*, 156.

Fonseca, I. C. (2020). Local E-Governance and Law: Thinking About The Portuguese Charter for Smart Cities: Challenges. In *IUS Publicom Network Review* (Issue n. 2). IUS Publicum Network review. http://www.ius-publicum.com/repository/uploads/29_07_2021_17_43_5_Fonseca_Ius_Publicum.pdf

International Organization for Standardization - ISO. (n.d.). *ISO/IEC 27002:2022(en), Information security, cybersecurity and privacy protection — Information security controls*. Retrieved May 14, 2022, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C. & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers and Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

NCSC, N. C. S. C. (2021). *Connected Places: Cyber Security Principles*.

Osório De Barros, G. (2018). A Cibersegurança em Portugal. In Ministério da Economia (Ed.), *Temas Económicos - GEE* (Temas Econ, Vol. 56, Issue 351). Gabinete de Estratégias e Estudos. https://www.sgeconomia.gov.pt/ficheiros-externos-sg/gee-ciberseguranca-pdf.aspx

Reyes-Menendez, A., Saura, J. R., & Palos-Sanchez, P. (2020). Cybersecurity and the Internet of Things: Anticipating the Leverage of Cyber Crimes with Interconnected Devices. In *The Evolution of Business in the Cyber Age*, 263–291. https://doi.org/10.1201/9780429276484-11

Sharif, R. A., & Pokharel, S. (2022). Smart City Dimensions and Associated Risks: Review of literature. Sustainable Cities and Society, 77, 103542. https://doi.org/10.1016/j.scs.2021.103542

Wirtz, B. W., & Weyerer, J. C. (2016). Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats. International Journal of Public Administration, *40*(13), 1085–1100. https://doi.org/10.1080/01900692.2016.1242614

DOCUMENTO ANEXO

INQUERITO DE VERIFICAÇÃO DA CIBERSEGURANÇA NAS ORGANIZAÇÕES PÚBLICAS MUNICIPAIS

Seção I - Estrutura de Segurança Organizacional

1. A organização possui uma unidade interna com competências específicas em segurança cibernética?

   No caso de uma resposta afirmativa à pergunta anterior:
2. Quantas pessoas esta unidade possui?
3. Foi designado um Ponto de Contato Permanente para assegurar o fluxo de informações a nível operacional e técnico com o Centro Nacional de Segurança Cibernética?
4. Foi designado um responsável para gerenciar todos os requisitos de segurança e medidas de comunicação de incidentes?

Seção II - Gestão de Ativos de TI

5. A organização possui um inventário atualizado de todos os bens de TI essenciais para seus serviços?

   No caso de uma resposta afirmativa à pergunta anterior:
6. O inventário foi validado e assinado pelo responsável pela Segurança?
7. O inventário foi comunicado ao Centro Nacional de Segurança Cibernética?
8. É mantida uma relação entre cada ativo, sua parte responsável e seu uso?
9. A gestão de ativos é conduzida utilizando uma abordagem simplificada e automatizada que reduz a burocracia?
10. Os serviços e funções críticas prioritárias da organização estão definidos e associados à tecnologia?
11. As contas de acesso interno e externo estão devidamente catalogadas?
12. O valor que essas contas poderiam representar para um agente malicioso em potencial é estimado?
13. A organização possui mecanismos internos para rastrear as "pegadas digitais" de seus funcionários e agentes com acesso particularmente privilegiado?
14. A organização possui documentação interna relativa a seus fornecedores e ativos de TI?
15. A organização possui mecanismos internos que podem facilitar a identificação de bens desconhecidos e reduzir as chances de perda de algo?
16. A organização tem um plano para validar seu sistema de gestão de ativos?
17. A organização tem políticas e procedimentos internos para desativar qualquer sistema ou informação que não seja mais utilizada ou necessária?

Seção III - Gerenciamento de Riscos Cibernéticos

18. A organização realiza uma análise de risco para todos os ativos que garantem a operação contínua das redes e sistemas de informação?

    No caso de uma resposta afirmativa à pergunta anterior:
19. Esta análise abrange, em relação a cada ativo a identificação de ameaças, internas ou externas, intencionais ou não intencionais, incluindo, nomeadamente:

(i) falha do sistema; (ii) fenômeno natural; (iii) erro humano; (iv) ataque malicioso; (v) falha no fornecimento de bens ou serviços por um terceiro. (vi) a caracterização do impacto e da probabilidade de tais ameaças?

20. Esta análise leva em consideração: O histórico de situações extraordinárias que ocorreram? O histórico de incidentes e incidentes com impacto relevante? O número de usuários afetados pelos incidentes? A duração do incidente? A distribuição geográfica em termos da área afetada pelos incidentes? As dependências intersectoriais para a prestação de serviços? A avaliação integrada de risco para a segurança de redes e sistemas de informação em nível nacional, europeu e internacional (publicada anualmente ou notificada à organização pelo National Cyber Security Center)?
21. A organização implementa medidas técnicas e organizacionais apropriadas para gerenciar os riscos identificados através da análise acima?
22. A organização documenta todas as informações relativas à preparação, execução e apresentação de tais análises?
23. A organização possui um plano de segurança?

No caso de uma resposta afirmativa à pergunta anterior:

24. El**e** está devidamente documentada e assinada pelo oficial de segurança?
25. Ele contém a política de segurança com uma descrição das medidas organizacionais e treinamento de recursos humanos? Uma descrição de todas as medidas tomadas em relação às exigências de segurança e comunicação de incidentes? A identificação do responsável de segurança? A identificação do Ponto de Contato permanente?
26. É revisado e, se necessário, atualizado de acordo com a evolução do contexto operacional da organização e a ocorrência de incidentes?
27. A segurança cibernética é considerada em outras políticas da organização?
28. A forma como as pessoas são apoiadas quando interagem com tecnologia, sistemas e serviços é segura e utilizável?
29. As pessoas contribuem para a gestão dos riscos de cibersegurança da organização?
30. As ferramentas, métodos, estruturas e normas, regras ou regulamentos utilizados pela organização para obter informações sobre os riscos associados a seus sistemas e serviços estão catalogados?
31. As estratégias de contra-ataque baseadas na Internet são as mais comuns?
32. São estabelecidas parcerias com outras entidades para compartilhar conhecimentos em segurança cibernética?
33. Os riscos cibernéticos identificados pela organização são comunicados efetivamente a seus funcionários e agentes?
34. São empregados controles para mitigar estes riscos?
35. Os trabalhadores e agentes são encorajados a liderar ações de segurança cibernética pelo exemplo?
36. Os altos funcionários do Condado seguem as políticas de segurança e não solicitam "tratamento especial" em relação à instalação de dispositivos ou acessos não padronizados?
37. A equipe de segurança entra em contato com os outros departamentos para compreender seu trabalho diário?

38. A perspectiva, o fluxo de trabalho e as pressões são compreendidas para saber quais são as barreiras à realização de certas atividades?
39. As pessoas com experiência e conhecimento sobre o funcionamento interno da organização estão incluídas no processo de formulação de políticas de segurança?
40. A organização tem procedimentos internos para relatar questões relacionadas à cibersegurança dentro da organização?
41. A organização prepara um Relatório Anual que, para o ano civil ao qual se refere, inclui os seguintes elementos? Principais atividades desenvolvidas em segurança de redes e serviços de informação; estatísticas trimestrais de todos os incidentes (número e tipo); análise de incidentes com impacto relevante (número de usuários afetados, duração dos incidentes, área afetada pelo incidente); recomendações para melhorar a segurança de redes e sistemas de informação; problemas identificados e medidas implementadas; quaisquer outras informações relevantes.

No caso de uma resposta afirmativa à pergunta anterior:

42. Tal relatório é enviado ao Centro Nacional de Proteção de Dados?
Existem campanhas de conscientização realizadas em segurança cibernética?
43. Há treinamento em segurança cibernética de acordo com as necessidades da organização?
44. No caso de uma resposta afirmativa à pergunta anterior:
45. Os funcionários e agentes da organização estão envolvidos na estruturação de tal treinamento para melhor adaptar seu conteúdo à realidade da instituição?
46. Esse treinamento é ministrado com frequência?
47. O conteúdo destes treinamentos é pequeno e fácil de ser assimilado?
48. Os participantes destes treinamentos contribuem para melhorar o treinamento futuro?
49. Estes treinamentos são apoiados pela gerência?
50. Os instrutores escolhidos possuem conhecimentos adequados sobre o assunto e como adaptá-lo à realidade da instituição?

Seção IV - Arquitetura e Configuração

51. A organização está ciente de seus riscos (ou não está) disposta a aceitá-los antes de projetar um sistema?
52. A organização tem um modelo de ameaça para seus sistemas?
53. Os sistemas e componentes mais críticos da missão da organização estão identificados?
54. É considerada a vida útil esperada dos sistemas da cidade?
55. Antes do projeto de um sistema, é realizada uma análise de mercado para verificar se produtos ou serviços equivalentes oferecem melhores garantias de segurança?
56. Ao implantar serviços computadorizados, é considerado o uso de um modelo de responsabilidade compartilhada para serviços em nuvem?
57. As configurações seguras são aplicadas a servidores e dispositivos de usuário para restringir as opções disponíveis a um agente malicioso em potencial?

58. Os dados de fontes externas ou menos confiáveis são transformados, validados ou processados de forma segura para que não possam ser usados para criar um ataque contra os sistemas da organização?
59. Os e-mails de domínio são dificultados para que não possam ser falsificados?
60. Os controles anti-spoofing são empregados para evitar o phishing convincente?
61. Nossos sistemas e serviços são projetados para serem seguros por padrão?
62. Os usuários podem utilizar algum método para contornar as medidas de segurança identificadas e catalogadas?
63. Os controles de segurança escolhidos são eficazes para mitigar os riscos?
64. Uma auditoria independente validou os controles mais críticos?
65. Os componentes críticos da rede, dados e comunicações estão isolados através de redes segregadas ou de uma arquitetura de "confiança zero"?

Seção V - Gerenciamento de vulnerabilidades

66. As atualizações automáticas estão disponíveis para sistemas operacionais e software?
67. Serviços gerenciados como soluções de Software as a Service (SaS) de fornecedores com um histórico comprovado em segurança utilizada?
68. São realizados estudos de priorização da vulnerabilidade?
69. Há planos alternativos de mitigação de vulnerabilidades mais difíceis de serem corrigidas?
70. Os métodos de testes manuais (testes de penetração ou exercícios de "equipe vermelha") são ferramentas definidas e automatizadas?

Seção VI - Gerenciamento da Identidade e Controle de Acesso

71. As políticas e procedimentos de gerenciamento de identidade e acesso foram definidos?
72. O controle é exercido sobre quem pode aceder dados e sistemas? Foram definidos métodos apropriados para estabelecer e provar a identidade dos usuários, dispositivos ou sistemas com confiança suficiente para tomar decisões de controle de acesso?
73. Foram estabelecidos acordos de não-divulgação com terceiros se eles precisarem ter acesso a seus sistemas?
74. Os acessos concedidos a terceiros são revogados quando não são mais necessários?
75. A alta administração tem contas de usuário separadas para suas atividades diárias (navegação na web ou clientes de e-mail) e outras atividades que requerem privilégios de acesso?
76. Existem processos definidos para controlar as contas de usuários e sistemas para revogar o acesso privilegiado quando não for mais necessário?
77. Existem monitores de segurança para detetar possíveis comportamentos maliciosos?
78. Os eventos de autenticação e autorização são registrados e monitorados para identificar comportamentos suspeitos que possam indicar comprometimento?
79. Existem sistemas de controle de acesso que permitem o fácil monitoramento do uso da conta de cada usuário?
80. As contas temporárias são removidas ou suspensas quando não são mais necessárias?

81. A autenticação multifatorial protege todas as contas de usuários?
82. A autenticação "user to service", "user to the device", e "device to service" é empregada?
83. Existe uma política de senha que equilibre adequadamente "usabilidade" e "segurança"?
84. A organização possui controles de acesso físicos e lógicos para que somente usuários autorizados possam aceder e modificar dados?

Seção VII - Segurança de Dados Corporativos

85. Os dados da organização são protegidos de acordo com os riscos identificados?
86. Os dados em trânsito são protegidos para garantir que não sejam vistos ou intercetados de forma inadequada?
87. As comunicações são criptografadas?
88. Os protocolos de aplicação seguros, criptografados e autenticados são utilizados sempre que possível?
89. A criptografia de camada de rede, como VPNs (Virtual Private Networks), é utilizada quando necessário?
90. As interfaces que permitem o acesso a dados confidenciais estão bem definidas?
91. As interfaces apresentam apenas as funcionalidades necessárias para reduzir as oportunidades de abuso por agentes maliciosos?
92. O monitoramento é conduzido para detetar compromissos, evitar consultas incomuns e tentativas de exportação de dados em massa?
93. Existe uma política de retenção de backups por pelo menos "um mês" para dados críticos?
94. Os backups são avaliados regularmente para garantir que possam ser efetivamente restaurados, caso surjam?
95. As aplicações executáveis podem ser restauradas a partir do código fonte, no caso de aplicações executáveis?
96. É aplicado um modelo hierárquico para contas de usuários?
97. A concessão de contas com privilégios totais só é feita quando necessário?
98. As etiquetas ou marcas indicando a propriedade do dispositivo (ou a natureza dos dados) são removidas antes da eliminação?
99. Os procedimentos e equipamentos de destruição intencional de dados são avaliados periodicamente?

Seção VIII - Registro e Monitoramento

100. Os objetivos pretendidos de registro e monitoramento a serem realizados pela organização estão claramente definidos?
101. O monitoramento se mostra proporcional ao contexto do sistema, às ameaças potenciais enfrentadas pela instituição e aos recursos disponíveis?
102. Há necessidade de um centro de operações de segurança (SOC) para detetar e responder a ataques avançados?
103. Existem estratégias de monitoramento interno definidas?
104. Há registros de monitoramento disponíveis para revisão quando eles precisam ser acedidos?
105. Os registros de monitoramento são mantidos por tempo suficiente para responder a perguntas que possam ser feitas durante um incidente?

106. Os registros utilizados nos registros de monitoramento estão definidos?
107. Existe um local centralizado para a análise dos conjuntos de dados?
108. O monitoramento garante que os logs sejam obtidos como esperado?
109. Existem registros de monitoramento para proteger contra adulterações?
110. O serviço de monitoramento analisa os registros para verificar se as políticas são aplicadas ou seguidas como esperado?
111. O sistema de monitoramento permite alertas de deteção baseados em ameaças antecipadas?

Seção IX - Gerenciamento de Incidentes

112. Existe um plano de resposta a incidentes e ele inclui o plano de continuidade de negócios, o plano de contingência, o plano de recuperação em caso de desastre e o plano de gerenciamento de crise?
113. A organização possui procedimentos internos para notificar o Centro Nacional de Segurança Cibernética de incidentes com impacto relevante ou substancial, de acordo com os artigos 15, 17 e 19 do Regime Jurídico de Segurança Cibernética?
114. O sistema utilizado pela organização permite que lições aprendidas de incidentes reais do passado sejam incorporadas em suas soluções de monitoramento?
115. O plano de gerenciamento de incidentes está alinhado com a estratégia de registro e monitoramento?
116. É usada a inteligência de ameaças?
117. A organização está inscrita no CiSP (Cybersecurity Information Sharing Partnership) para receber e compartilhar informações sobre ameaças?
118. A equipe de resposta ao incidente integra os colaboradores? da área de Segurança da Tecnologia da Informação; do Departamento Jurídico; de Recursos Humanos; da área de Relações Públicas; de outras áreas?
119. Os papéis e responsabilidades de todos os envolvidos no plano de resposta ao incidente estão definidos e compreendidos?
120. Foi fornecido treinamento adequado para a equipe de gerenciamento de incidentes?
121. Existem planos de resposta a incidentes alinhados com todos os métodos de deteção pré-definidos?
122. O plano de resposta ao incidente inclui orientação sobre requisitos legais ou regulamentares com base nos tipos e volumes de dados da instituição?
123. Existem simulações dos planos de resposta aos incidentes realizados para verificar sua eficácia?
124. Existe um plano de comunicação definido com as partes interessadas para ser usado durante um incidente?
125. Os registros da resposta ao incidente, decisões, ações tomadas e dados capturados (ou em falta) são coletados para análise posterior?

Seção X - Cadeia de Suprimentos

126. A organização tem uma imagem clara de sua cadeia de abastecimento?
127. As responsabilidades de segurança de cada ator da cadeia estão definidas e são satisfatórias para todas as partes envolvidas?
128. A dimensão da segurança é considerada um fator de contratação?

129. Ao contratar serviços na nuvem, a existência de informações publicadas pelos fornecedores em seus websites é avaliada para ajudar a entender se eles oferecem níveis adequados de segurança?
130. A organização fornece orientação, ferramentas e processos de apoio aos fornecedores para gerenciar eficazmente os riscos da cadeia de suprimentos de acordo com suas necessidades?
131. Os contratos estabelecidos com fornecedores definem claramente os requisitos específicos para a devolução e eliminação de informações e ativos após o término desse contrato?
132. Os acordos baseados em fornecedores incluem requisitos para gerenciamento e comunicação de incidentes de segurança?
133. Existe um canal de comunicação definido para ouvir e responder a quaisquer preocupações levantadas pelo monitoramento de desempenho, incidentes ou relatórios de fornecedores que sugerem que as abordagens não estão funcionando tão eficazmente quanto planejado?