Guia de cibersegurança para cidades inteligentes

AUTORES: Lorenzo **Cotino**
Marco **Sánchez**

EDITORES: Mauricio **Bouskela**
Gilberto **Chona**
Ariel **Nowersztern**
Patricio **Zambrano-Barragán**
Isabelle **Zapparoli**

BID

Guia de cibersegurança para cidades inteligentes

Autores:
Lorenzo Cotino
Marco Sánchez

Editores:
Mauricio Bouskela
Gilberto Chona
Ariel Nowersztern
Patricio Zambrano-Barragán
Isabelle Zapparoli

Banco Interamericano de Desenvolvimento

Dezembro de 2021

Catalogação na fonte fornecida pela
Biblioteca Felipe Herrera do
Banco Interamericano de Desenvolvimento

Guia de cibersegurança para cidades inteligentes / Lorenzo Cotino, Marco Sánchez; editores, Maurício Bouskela, Gilberto Chona, Ariel Nowersztern, Patricio Zambrano-Barragán, Isabelle Zapparoli.
p. cm. — (Monografia do BID ; 963)
Inclui referências bibliográficas.
1. Smart cities-Latin America. 2. City planning-Technological innovations-Latin America. 3. Computer security-Latin America. 4. Computer crimes-Latin America-Prevention. I. Cotino Hueso, Lorenzo. II. Sánchez, Marco. III. Bouskela, Maurício, editor. IV. Chona, Gilberto, editor. V. Nowersztern, Ariel, editor. VI. Zambrano-Barragán, Patricio, editor. VII. Zapparoli, Isabelle, editora. VIII. Banco Interamericano de Desenvolvimento. Divisão de Habitação e de Desenvolvimento Urbano. IX. Banco Interamericano de Desenvolvimento. Divisão de Inovação para Servir ao Cidadão. X. Série.
IDB-MG-963

Códigos JEL: J18, K24, L86, L88, L90, L94, L95, L96, L98, M15, N96, O14, O18, O19, O31, O32, O38

Palavras-chave: Cibersegurança, segurança cibernética, segurança digital, ciberataques, ataques cibernéticos, ataques digitais, ciberespaço, espaço cibernético, espaço digital, proteção de dados, governança, proteção de ativos, cidades, cidade inteligente, cidades inteligentes, smart city, smart cities, sistemas de informação, tecnologia da informação, Internet das coisas, IoT, infraestrutura urbana, serviços urbanos, América Latina e Caribe, ALC, segurança da informação, segurança de TI, transformação digital, diretor de segurança da informação, CISO.

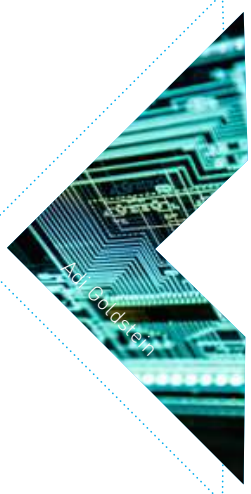
Este guia de cibersegurança para cidades e governos subnacionais oferece conhecimentos e recomendações para ajudar as cidades da América Latina e do Caribe (ALC) a se protegerem no espaço cibernético. O guia se destina aos governantes municipais, gestores e servidores municipais e técnicos da área de TIC, e está dividido em cinco partes. Primeiro, ele aborda temas gerais da cibersegurança e os principais aspectos que a constituem, inclusive atores, riscos e impactos. Em segundo lugar, o guia traz um roteiro introdutório à cibersegurança no nível local. Em terceiro lugar, é apresentada uma série de recomendações voltada aos três principais públicos-alvo da administração local. Em quarto lugar, ele detalha informações e referências sobre modelos de gestão de riscos, ferramentas e outros instrumentos úteis para o pessoal técnico de TIC dos municípios. Finalmente, são apresentadas a contribuição do BID sobre o tema e as conclusões.

https://www.iadb.org

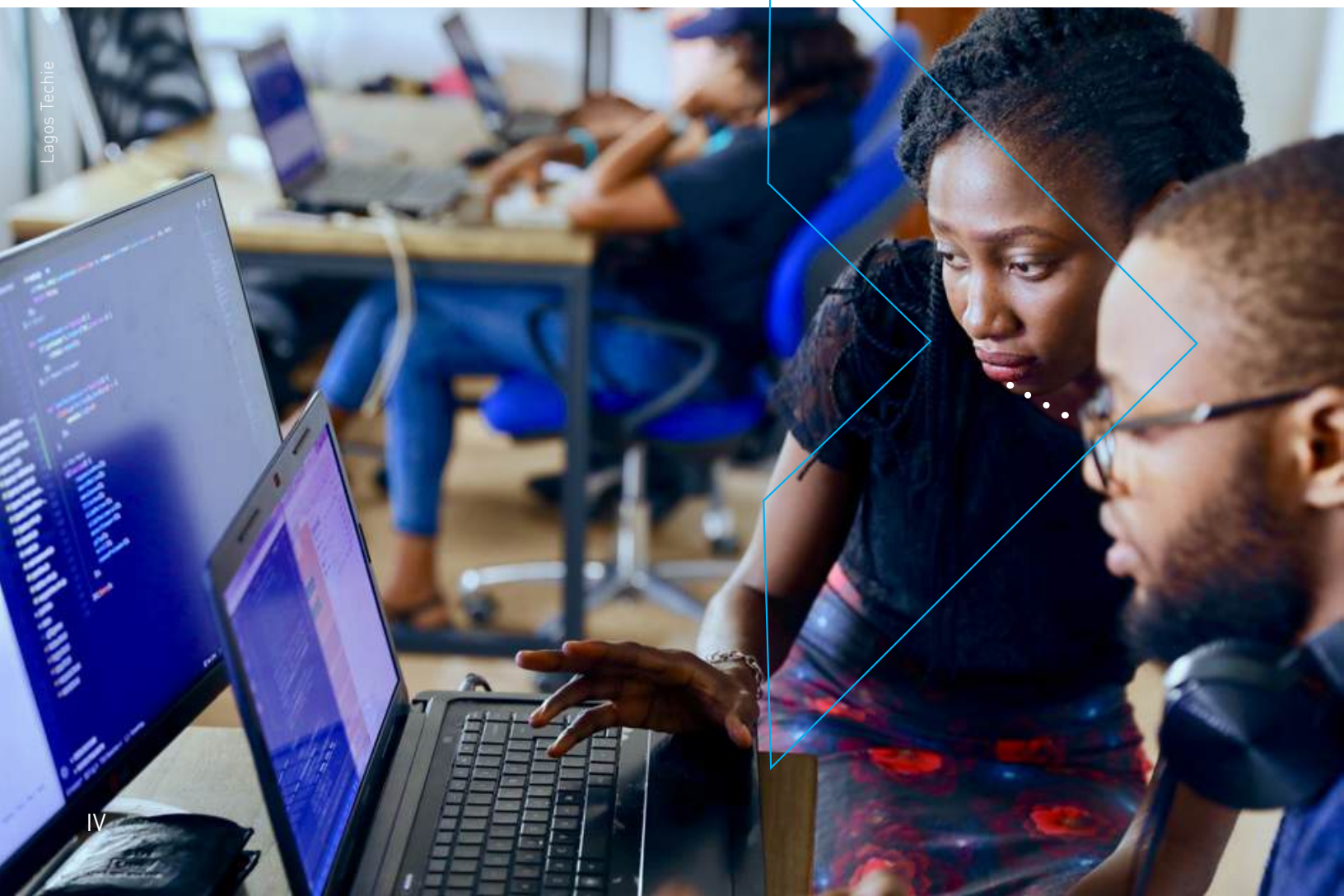
Tradução: Marsel de Souza

Revisão: Sarah Schineller e Márcio Henrique Badra

Desenho gráfico: Ramón Zamora



Este guia de cibersegurança para cidades inteligentes visa fornecer conhecimento e valor agregado para entender melhor a cibersegurança, riscos, impactos potenciais e a urgência de agir proativamente para proteger as cidades da América Latina e do Caribe.



Sumário

Adam V

Prefácio

Román López

"Este guia de cibersegurança para cidades inteligentes é uma contribuição inicial para uma discussão emergente que nos levará a respostas consistentes e contundentes ao desafio que a cibersegurança representa para o desenvolvimento resiliente, sustentável e equitativo de nossas cidades."

Prefácio

A digitalização é um componente fundamental da "Visão 2025[1]: Reinvestir nas Américas" do Banco Interamericano de Desenvolvimento (BID) e se baseia na ideia de que aproveitar ao máximo o imenso potencial da transformação digital requer pensamento estratégico de longo prazo, melhor conectividade, fortalecimento da governança digital, estímulo à inovação, ampliação do capital humano, uma infraestrutura digital mais sólida e a atualização de legislações obsoletas que regem as tecnologias da informação e comunicação (TICs).

Com o advento da pandemia de COVID-19, o processo de digitalização global se acelerou consideravelmente, trazendo consigo mudanças importantes na forma de viver, trabalhar e comunicar-se. A digitalização aumentou nas empresas, residências e serviços públicos.

Foram introduzidas novas formas de acesso à informação e aos serviços, foram abertos novos canais de comunicação entre o governo e os cidadãos e foram oferecidas oportunidades para a melhoria da governança em geral.

As regiões metropolitanas e os municípios não estão alheios a essa mudança do paradigma digital. Com efeito, as cidades são um agente cada vez mais importante no processo de digitalização mundial. A adoção das novas tecnologias digitais é uma característica essencial para o desenvolvimento das cidades e um vetor de inovação, ampliação da comunicação, colaboração, equidade e eficiência.

Entretanto, com o crescimento da digitalização da gestão pública local, da infraestrutura e dos serviços urbanos, aumentam também a exposição ao risco e a vulnerabilidade a ataques cibernéticos. Ou seja, a dependência das TICs para gerir e monitorar sistemas essenciais que sustentam áreas primordiais como segurança, água, energia, mobilidade e rastreamento de ocorrências catastróficas relacionadas à mudança do clima aumenta os níveis de risco de ataques cibernéticos.

1. Ver https://www.iadb.org/pt/sobre-o-bid/visao-geral.

A cibersegurança das cidades logo se transformou em um elemento indispensável para sua boa governança. Os ataques cibernéticos têm potencial elevado para interromper as operações das cidades, afetar suas finanças e a reputação do poder público e causar danos significativos aos sistemas de informação por tempo indeterminado. Entre outras áreas críticas, esses ataques cibernéticos ameaçam a continuidade dos serviços, o acesso ágil à informação, a privacidade dos dados pessoais e os meios digitais de pagamento empregados pelos municípios e pelos cidadãos.

As cidades continuam inevitavelmente expostas a falhas de cibersegurança. Embora muitas cidades tenham sido alvo de ataques cibernéticos, ainda continuam a existir desafios e dificuldades na governança e gestão do risco para abordar a cibersegurança de forma proativa, sobretudo no nível municipal.


Goh Rhy Yan

Os dados disponíveis indicam um claro aumento na frequência e sofisticação dos ataques e incidentes cibernéticos, principalmente aqueles perpetrados com intenção criminosa, que podem ter custos muito elevados. Além disso, a criminalidade cibernética não reconhece as fronteiras nacionais e constitui um problema que afeta todas as entidades dos setores público (nacional ou subnacional) e privado.

Recentemente, o BID realizou esforços importantes para equacionar as falhas de conhecimento sobre cibersegurança e ajudar os órgãos públicos nacionais e as empresas privadas a melhorar suas estruturas, medidas e capacidades para fortalecer a cibersegurança, em conjunto com a necessidade de aprofundar a cooperação e o intercâmbio de informações.

Os principais desafios para fazer frente à vulnerabilidade das cidades aos crimes cibernéticos estão relacionados à governança debilitada e à falta de consciência sobre a gravidade dos riscos e o potencial de danos de um possível ataque cibernético. Além disso, a destinação de recursos limitados em um contexto de restrição orçamentária face a múltiplas prioridades, assim como a falta de recursos humanos qualificados, exacerbam a gravidade do problema.

Para as cidades da região, a questão não é "se" irá acontecer um ataque cibernético, mas sim "quando" ele ocorrerá. As cidades podem se planejar de forma proativa para que os ataques cibernéticos não desestabilizem sua governança e suas atividades administrativas.
.

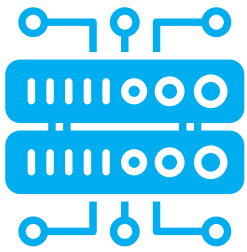
A análise da cibersegurança nas cidades apresentada nesta publicação tem o intuito de promover o conhecimento e as ações de proteção digital para as cidades da América Latina e do Caribe (ALC), por meio de uma abordagem franca e aberta do assunto, de tal modo que sirva de guia introdutório para que os decisores municipais fortaleçam seu processo de digitalização e reduzam a vulnerabilidade a ataques cibernéticos.

Em termos específicos, este guia ajudará a promover a conscientização sobre a importância de consolidar as estruturas e processos de cibersegurança das cidades; entre outras ferramentas, ele propõe, em termos concretos, um roteiro e um plano de ação necessários para as cidades da ALC.

Este guia de cibersegurança para cidades constitui uma contribuição inicial para uma nova discussão que nos levará a respostas coerentes e categóricas diante do desafio representado pela cibersegurança para o desenvolvimento resiliente, sustentável e equitativo de nossas cidades. Almejamos melhorar a vida em cidades cada vez mais digitalizadas e queremos fazer isso com segurança.

Tatiana Gallego Lizón
Chefe da Divisão de Habitação e Desenvolvimento Urbano
Setor de Mudanças Climáticas e Desenvolvimento Sustentável
Banco Interamericano de Desenvolvimento

Edgardo Mosqueira Medina
Chefe da Divisão de Inovação para Atender ao Cidadão (a.i.)
Setor de Instituições para o Desenvolvimento
Banco Interamericano de Desenvolvimento



Prólogo e agradecimentos

Jurriaan

"Cada vez mais, os governos municipais lançam mão da tecnologia digital, da Internet e da tecnologia de telefonia celular para planejar, conectar e gerir a infraestrutura e os serviços urbanos e, assim, melhorar a qualidade de vida de seus habitantes."

Prólogo e agradecimentos

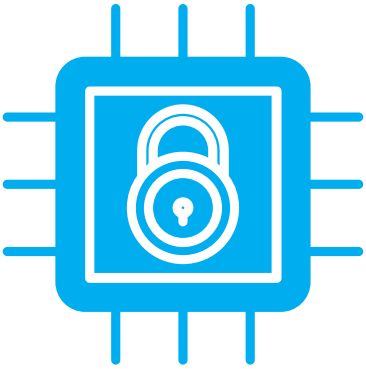
Este guia nasceu da reflexão do BID sobre como auxiliar as cidades da região para que se protejam no ciberespaço enquanto convertem sua gestão tradicional para um modelo inteligente.

Cada vez mais, os governos municipais lançam mão da tecnologia digital, da Internet e da tecnologia de telefonia celular para planejar, conectar e gerir a infraestrutura e os serviços urbanos e, assim, melhorar a qualidade de vida de seus habitantes. A pandemia acelerou a digitalização das cidades. Cidades mais conectadas são sinônimo de cidades mais expostas. O risco de virar alvo de ataques cibernéticos é cada vez maior. O custo econômico de paralisar o funcionamento da cidade é muito alto e coloca em risco não apenas a infraestrutura e os serviços urbanos, mas também a segurança dos cidadãos.

A elaboração deste guia foi um esforço conjunto dos setores de Mudanças Climáticas e Desenvolvimento Sustentável (CSD), Instituições para o Desenvolvimento (IFD) e Conhecimento, Inovação e Comunicação (KIC), capitaneados por Juan Pablo Bonilla, Moisés Schwartz e Federico Basañes, respectivamente. A supervisão técnica foi proporcionada pela Divisão de Habitação e Desenvolvimento Urbano (CDS/HUD) e pela Divisão de Inovação para Atender ao Cidadão (IFD/ICS), sob a responsabilidade de Tatiana Gallego Lizón e Edgardo Mosqueira Medina (a.i.), respetivamente. A coordenação ficou a cargo de Mauricio Bouskela, Gilberto Chona e Ariel Nowersztern, com o apoio de Isabelle Zapparoli, que editaram a versão original do texto em espanhol, com contribuições de Patricio Zambrano-Barragán e Miguel Ángel Porrúa como revisores de conteúdo e abordagem.

Os autores, Lorenzo Cotino Hueso (Espanha) e Marco E. Sánchez Acevedo (Espanha-Colômbia), são professores universitários e especialistas jurídicos em cibersegurança e uso de TICs pelas administrações públicas; com eles, a equipe de coordenação selecionou os temas determinantes, características e recomendações de cibersegurança, todos voltados para três públicos das administrações municipais: dirigentes municipais, gestores e servidores municipais e pessoal técnico de TIC.

A questão da cibersegurança tem muitas facetas; existem estudos de caso, modelos e âmbitos de ação. Contudo, nesta primeira edição, o guia sintetiza as questões críticas de cibersegurança nas quais os três públicos citados acima devem se concentrar.

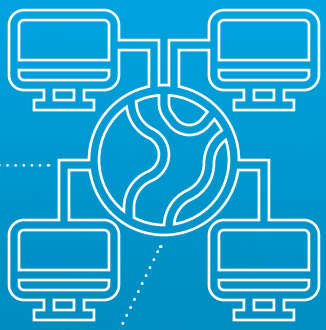


Este guia sobre cibersegurança para cidades inteligentes foi financiado com recursos do programa *Cutting-Edge* da divisão KIC (VPS/KIC). Agradecemos pelo apoio de Pablo Alzuri, Allen Blackman, Andrés Blanco, Janaina Borges, Hallel Elnir, Luis Manuel Espinoza, Andrea Florimon, Kenneth Foley, Jessica Guzmán Osorio, Cristina Hinojosa Lecaros, Philip Keefer, Kidae Kim, Pablo Libedinsky, Nora Libertun, Ángel Macuare Herrera, Marcelo Madeira da Silva, Fernando Melean, Santiago Paz, Daniel Peciña López, Lorena Rodríguez Bu e Sarah Schineller pelo assessoramento e apoio durante o desenvolvimento da proposta, financiamento, processos internos e comunicação estratégica relacionados com a publicação.

A equipe agradece aos gestores e equipes técnicas das cidades da ALC, que, ao longo dos anos, por meio do diálogo, da execução de projetos e da participação em estudos, compartilharam conosco sua preocupação em melhorar os serviços nas cidades e nos ajudaram a gerar conteúdo para a agenda de política urbana da região.

Ma Zhang

Introdução



Marck Maciel

"As cidades usam cada vez mais o ciberespaço, uma infraestrutura complexa de redes de conectividade e interfaces de comunicação, sensores e dispositivos conectados, além de centros de operação e controle."

Introdução

O BID apresenta este guia com o objetivo de promover a conscientização e a compreensão da segurança cibernética, ou cibersegurança, bem como os possíveis riscos e resultados dos ataques cibernéticos às operações das cidades. O guia permite visualizar os riscos, possíveis impactos e urgência da gestão da proteção das cidades da região contra esses ataques.

A cibersegurança deve ocupar posição de destaque na agenda dos dirigentes municipais e dos governos nacionais, regionais e locais.

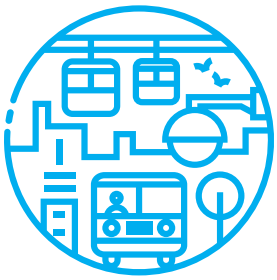
O que é o Guia de Cibersegurança para Cidades Inteligentes?


Martin Adams

Este guia de cibersegurança para cidades e governos subnacionais (que chamaremos de "governos") oferece conhecimento para as cidades da ALC sobre cibersegurança, riscos digitais, possíveis impactos e a urgência de ação proativa.

Esse guia faz parte do apoio que o BID oferece às cidades da ALC em sua transformação digital, e é um complemento a outras publicações, inclusive as seguintes: Caminho para as smart cities: Da gestão tradicional para a cidade inteligente (2016); Big Data urbana: una guía estratégica para ciudades (2019); Políticas Públicas Orientadas por Dados: os Caminhos Possíveis para Governos Locais (2020) y Big Data para o Desenvolvimento Urbano Sustentável (2021).

Além disso, o guia integra o acervo de conhecimento especializado estendido pelo BID sobre a questão emergente da cibersegurança em diferentes setores, inclusive energia, saúde, recursos hídricos e aplicação da lei, com os quais procura colaborar para eliminar o déficit de conhecimento que impede seu desenvolvimento digital. Na publicação Relatório de Cibersegurança 2020: Riscos, Avanços e o Caminho a Seguir na América Latina e Caribe, o BID, e a Organização dos Estados Americanos (OEA), descrevem em detalhes o grau de maturidade em cibersegurança dos países da ALC, bem como as oportunidades de melhoria.



A quem se destina este guia?

O **Guia de Cibersegurança para Cidades Inteligentes** é voltado para três tipos de usuários das cidades (ver Figura 1).

Figura 1.

Usuários do Guia de Cibersegurança para Cidades Inteligentes

Fonte: Elaboração própria (2021).

Quais são os objetivos deste guia?

Os objetivos do guia são:

1. **Ajudar as cidades** e governos municipais da região da ALC a se protegerem no espaço digital.
2. **Promover a conscientização** e compreensão da cibersegurança a fim de assegurar a proteção da informação de cada cidade e a continuidade dos serviços e infraestrutura.
3. **Proporcionar conhecimentos** sobre os possíveis riscos e a adoção de medidas de segurança para reduzir a probabilidade de ataques cibernéticos, bem como minimizar o impacto em caso de incidente.

Markus Spiske

Como este guia está organizado?

O Guia de Cibersegurança para Cidades é dividido em cinco capítulos, que servem de orientação para que os dirigentes governamentais, gestores municipais e pessoal técnico responsável pela cibersegurança e pelas TICs, bem como terceiros, transformem efetivamente suas municipalidades em cidades seguras e inteligentes.

A seguir, apresentamos um sumário executivo, que contém a estrutura essencial dos elementos abordados ao longo do documento. Primeiramente, o capítulo 1, traz uma definição de cibersegurança em contexto e uma descrição do ecossistema, motivações, atores, ameaças, vulnerabilidades e impacto que um ataque pode gerar no nível municipal. No capítulo 2, são abordadas as melhores práticas, roteiro, governança, institucionalização da cibersegurança, relação com a cadeia de suprimentos, bem como a formação, cultura e financiamento de projetos nessa área. O capítulo 3, apresenta um conjunto de recomendações destinadas ao pessoal estratégico, tático e operacional, técnico e pessoal terceirizado de apoio para enfrentar as ameaças geradas pelas atividades mediadas pelas TICs. O capítulo 4, explica as capacidades técnicas necessárias para o provimento de cibersegurança às cidades. O capítulo 5, apresenta o escopo de ação do BID em cibersegurança no contexto da promoção da digitalização da região e das cidades inteligentes.

Sumário Executivo

Fabio Hanashiro

"A cibersegurança ideal é invisível, pois antecipa e elimina problemas."

Sumário Executivo

Os prefeitos e suas equipes municipais estão liderando a transformação digital das cidades com vistas a prestar serviços melhores e gerir a infraestrutura urbana, bem como melhorar a autonomia financeira, a sustentabilidade e a governabilidade.

As cidades usam cada vez mais o espaço digital, uma infraestrutura complexa de redes de conectividade e interfaces de comunicação, sensores e dispositivos conectados e de centros de operação e controle. Essa digitalização vem acompanhada de projetos de cidades inteligentes ou conectadas, inclusive com o uso de inteligência artificial e de novas tecnologias para a coleta e exploração de dados para monitorar, propor ou tomar decisões acerca das cidades ou dos cidadãos.

Porém, essa transformação digital está atraindo cada vez mais criminosos cibernéticos para as cidades, o que também se verifica na ALC. No entanto, a grande maioria dos prefeitos, executivos, servidores e a própria população não tem conhecimento das vulnerabilidades de cibersegurança das cidades. Centenas de milhares de ataques digitais ocorrem todos os dias. Felizmente, a maior parte é repelida graças às medidas de cibersegurança. Em algumas ocasiões, a população é impactada por notícias de furtos de dados da municipalidade, ataques a seus sistemas de transporte, emergência ou polícia, bem como a seus hospitais. Cidades inteiras já foram chantageadas e ficaram paralisadas durantes semanas (Baltimore), e já houve dezenas de servidores exonerados por não investir nessa área em tempo hábil (Atlanta). Ocorreram até episódios de violência urbana em decorrência de ataques de desinformação.

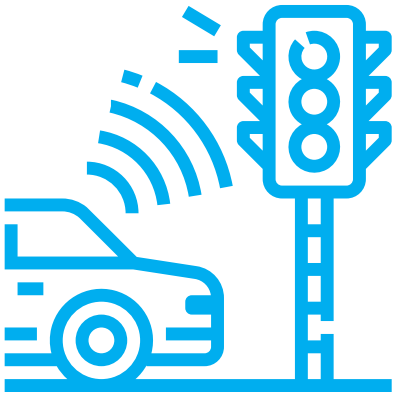
A cibersegurança ideal é invisível, pois antecipa e elimina problemas. Não se deve esperar que os desastres ocorram para se proteger. É preciso preveni-los e saber como agir caso ocorram. A interrupção de serviços públicos e infraestruturas críticas da cidade tem um custo social, econômico, político e de reputação muito alto para qualquer centro urbano.

Este guia tem por finalidade conscientizar e compreender as ameaças cibernéticas para poder passar à ação. Assim, oferece o que são considerados alguns dos melhores instrumentos e recomendações, um roteiro e elementos básicos para a ação proativa contra as ameaças digitais. O guia sinaliza o caminho para que dirigentes, prefeitos e gestores, além de servidores, técnicos e terceiros transformem suas cidades em lugares mais seguros.


Chuttersnap

O **primeiro capítulo** explica o conceito de cibersegurança ou digital, ameaças cibernéticas e o impacto dos ataques digitais a cidades. A cibersegurança supõe a proteção de dados, informações, *hardware, software*, serviços, recursos humanos, instalações e infraestrutura crítica. Ela envolve todos os atores de uma cidade inteligente, e por isso sua finalidade é reduzir os riscos ou ameaças cibernéticas a que autoridades, cidadãos e empresas estão expostos quando realizam suas atividades ou cumprem suas funções no meio digital.

Não é nada fácil saber porque os criminosos, espiões, terroristas, ativistas digitais ou quem quer que seja empreendem os ataques (contra instituições, governos, entidades privadas, empresas, outros países), nem quais são suas motivações (políticas, criminais, econômicas ou empresariais ou meramente pessoais). Estamos vulneráveis devido a falhas de *software*, infraestrutura muitas vezes obsoleta, por não conhecermos ou não entendermos nossas vulnerabilidades, ou não compreendermos o ecossistema tecnológico da cidade. Não é fácil governar e coordenar os diversos atores envolvidos, nem saber e compartilhar as informações sobre segurança e sobre incidentes ou falhas quando eles ocorrem. Os autores dos ataques tiram proveito da falta de estratégias, planos de gestão de riscos e de gestão de incidentes de suas vítimas. E as vulnerabilidades humanas geralmente são mais importantes do que as tecnológicas. Recursos humanos com os novos perfis profissionais exigidos não são conhecidos e muito menos contratados; os ataques ocorrem principalmente porque não há campanhas de conscientização ou sensibilização nem oferta de capacitação ou treinamento para gestores, servidores ou para a própria população.



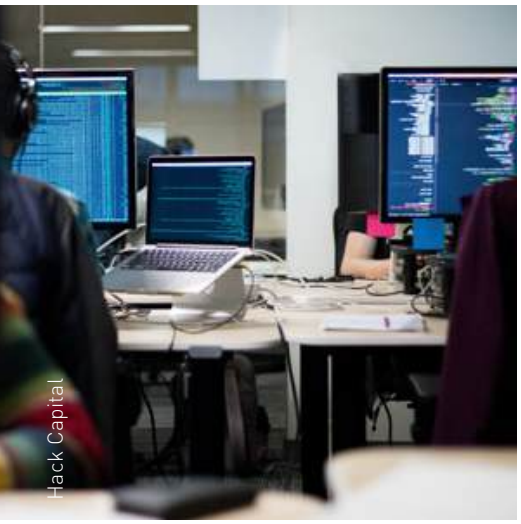
Esse capítulo descreve alguns ataques digitais ocorridos no mundo, e também na ALC, que paralisaram cidades e geraram custos elevados, chegando até a ocasionar a exoneração de governantes. Esses casos devem favorecer a conscientização sobre a importância da cibersegurança nas cidades e podem contribuir para convencer os gestores estratégicos, táticos e tecnológicos ou operacionais da necessidade de agir. A COVID-19 intensificou os ataques digitais. As vulnerabilidades aumentaram devido ao teletrabalho sem medidas de proteção suficientes e a novas formas de engenharia social, decorrentes das preocupações e necessidades geradas pela doença. Houve também centros e sistemas de saúde que foram atacados ou chantageados, entre outros tipos de crimes.

O **segundo capítulo** traz algumas recomendações e descreve boas práticas que constituem um possível roteiro que qualquer cidade pode seguir para alcançar a melhor cibersegurança possível. Além disso, são traçados os perfis dos responsáveis pela execução dessas ações. Tudo começa com a identificação dos ativos e dos

atores; devido à complexidade da cidade a ser protegida e aos numerosos intervenientes, faz-se necessária uma governança da cibersegurança integrada à governança da cidade inteligente e à governança de dados em termos mais abrangentes.

A segurança digital da cidade deve estar conectada, respaldada e articulada pelas políticas e estratégias nacionais de cibersegurança e deve ser institucionalizada. Esta não é a praxe. Contudo, uma cidade pode ser pioneira se cooperar proativamente na geração de conhecimento e incorporar as melhores práticas dos níveis internacional, nacional, regional e também local. Nesse caso, ela poderá também ter acesso aos melhores recursos e fontes de financiamento. A governança da cibersegurança parte da legislação a ser cumprida. Algumas leis específicas são mencionadas no guia; da mesma forma, é preciso conhecer os padrões de cibersegurança de referência e escolher o mais adequado e viável para a cidade. Com base nisso, o nível estratégico deve desenvolver políticas e normas de segurança para todos os atores e definir competências claras. Obviamente, todas as partes devem se mobilizar para apropriar-se dessas políticas e normas. Recomenda-se centralizar a responsabilidade pela cibersegurança em uma pessoa ou órgão.

O roteiro a seguir também implica que a segurança dos dados e informações deve ser pautada pelo seu nível de risco, o que é especialmente válido no caso dos dados confidenciais ou pessoais.


Hack Capital

Uma das maiores barreiras à cibersegurança é a falta de confiança ou de instrumentos e plataformas que permitam o compartilhamento de informações sobre segurança e incidentes entre as partes. Nesse sentido, apresentamos alguns modelos e boas práticas a serem seguidos para a organização e troca de informações.

A colaboração entre os setores público e privado é essencial para a transformação digital das cidades e também para sua cibersegurança. Por isso, este guia traz recomendações específicas para a integração da cibersegurança na contratação de fornecedores e na oferta de produtos e serviços tecnológicos para a cidade, com uma descrição específica dos serviços a serem incluídos, da atenção, das informações a serem compartilhadas, da obrigação de que os produtos e serviços incorporem a segurança desde sua concepção e do cumprimento das normas e regulamentos. Igualmente, são apresentadas uma série de recomendações úteis para a seleção da empresa ou prestador de serviços da cidade inteligente.

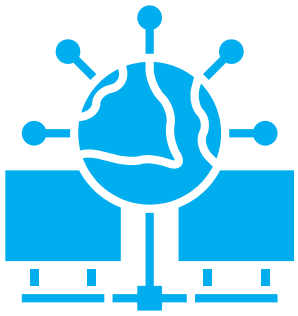
Conforme citado, o fator humano é ainda mais importante do que as medidas técnicas de cibersegurança. Portanto, é imprescindível uma cultura de segurança, conscientização e capacitação, em que tudo começa com o prefeito ou prefeita e sua equipe, passa pela alta administração e pelos responsáveis da cidade inteligente, além de todos os servidores e técnicos em tecnologia, e termina com a população como um todo. Recomenda-se dar ênfase especial à boa comunicação de todas as ações realizadas por todos os envolvidos. Por fim, não há dúvida de que a cibersegurança precisa de financiamento planejado, que inevitavelmente precisará ser ampliado se os recursos não forem alocados em tempo hábil. Aponta-se também a possibilidade de contratação de seguros para cibersegurança urbana.


Josh Hild

No **terceiro capítulo**, são propostos três decálogos para se alcançar a cibersegurança para os três perfis mencionados no início.

Em primeiro lugar, são apresentadas recomendações no **nível estratégico** (prefeitos e alta administração) em uma perspectiva urbana no médio e longo prazo; é enfatizada a necessidade de colocar o assunto na pauta de políticas, visando a destinação de recursos sem ter que esperar um ataque; finalmente, fortalecer as ações com normas, competências claras e a institucionalização de lideranças e órgãos que disponham de recursos adequados. Deve ser incentivada a colocação em prática das medidas preventivas, evitando que sejam "engavetadas". Deve ser exercida também liderança sobre os operadores do setor privado que fornecem bens e serviços para o município. É necessário monitorar a renovação de equipamentos obsoletos, que devem ser substituídos por novos equipamentos que ofereçam segurança nos meios digitais. A privacidade e a cibersegurança precisam ser integradas às avaliações da cidade inteligente, e é necessário adotar estratégias e aderir a redes nacionais e até internacionais de segurança nessa área.

É apresentado também um decálogo para o **nível tático** (secretários e servidores municipais). Nesse caso, é necessário um bom conhecimento dos sistemas e infraestruturas a serem protegidos e das principais ameaças que podem sofrer. Para tanto, a realização de uma autoavaliação é particularmente útil para determinar as capacidades ainda inexistentes. Ademais, os secretários municipais devem estar a par das ações, estratégias, normas, políticas e procedimentos concretos de cibersegurança que a cidade possui, além de ter clareza em relação a suas responsabilidades nesse campo e comunicar as responsabilidades que dizem respeito aos órgãos e servidores municipais. Da mesma forma, deve-se assegurar que as medidas previstas sejam testadas.



Os secretários devem receber capacitação adequada e contar com financiamento e recursos humanos estruturados, planejados e suficientes. Quanto aos provedores e prestadores privados, é necessário especificar as obrigações e, ao mesmo tempo, criar um clima de confiança que permita o compartilhamento de informações essenciais sobre cibersegurança.

Para o **nível operacional** (pessoal com responsabilidades ou tarefas relacionadas à tecnologia, pessoal com capacidades tecnológicas e pessoal externo de apoio) há também um decálogo, que inclui a determinação das informações e ativos a serem protegidos e a participação ativa na avaliação, gestão e planejamento da cibersegurança como um processo contínuo. O trabalho técnico desempenha um papel preponderante para que haja sistemas de identificação, autenticação forte de dois fatores, controle de acesso, mecanismos de detecção de anomalias e vigilância para responder a incidentes. Também deve-se assegurar que os bens e serviços incorporem de antemão os níveis de segurança e privacidade indicados no projeto. Da mesma forma, é importante estar atualizado em relação aos métodos e ferramentas dos criminosos, bem como contar com sistemas automatizados para detectar e responder às ameaças. Da mesma forma, é necessário assegurar que o *hardware* e o *software* estejam atualizados e integrar as ações de privacidade e proteção de dados com as de cibersegurança.

O **quarto capítulo** traz uma seção especificamente destinada aos gestores e especialistas em tecnologia. Assim, os aspectos técnicos da cibersegurança são agrupados com uma descrição do ciclo e etapas a seguir (gestão, identificação, proteção, detecção, resposta, recuperação e autoavaliação). São explicados, para um público de perfil tecnológico, os elementos técnicos do planejamento baseado em capacidades, bem como o roteiro e os principais modelos de maturidade das capacidades e funções de cibersegurança, equipamentos e tecnologia para gerir a segurança no dia a dia de uma cidade. Por fim, são detalhadas as responsabilidades a serem atribuídas a este grupo de alto nível encarregado da cibersegurança.

Finalmente, o **quinto capítulo** ilustra como o BID conjuga a cibersegurança com sua visão e âmbito de ação, com base na promoção das cidades inteligentes a serviço dos cidadãos. Em seguida é apresentada a síntese de uma série de conclusões gerais. Assim, destaca-se a essência da cibersegurança: conhecimento e compreensão do ambiente, planejamento, proatividade na prevenção e vigilância constante, colaboração e cooperação, treinamento e capacitação permanentes. Somente se forem observados esses princípios será possível aproveitar as vantagens das tecnologias inovadoras para ter cidades mais sustentáveis, inclusivas e produtivas e melhorar a vida dos cidadãos.

1 Cibersegurança, ameaças digitais e seu impacto na cidade

NASA

"A cibersegurança supõe a proteção de dados, informações, **hardware, software,** *serviços, recursos humanos, instalações e infraestrutura crítica."*

1 Cibersegurança, ameaças digitais e seu impacto na cidade

A partir do século 21, o uso das TICs passou a ser um elemento central das cidades, dos Estados e do exercício dos direitos dos cidadãos. Cada centro urbano deflagrou seu processo de transformação digital para alcançar o que foi chamado de cidade inteligente, ou *smart city*. Segundo Bouskela et al. (2016), uma cidade inteligente é aquela que coloca as pessoas no centro do desenvolvimento, incorpora as TICs na gestão urbana e emprega esses elementos como ferramentas para estimular a formação de um governo eficiente, que inclua processos de planejamento colaborativo e participação dos cidadãos. Ao promover o desenvolvimento integrado e sustentável, as cidades inteligentes se tornam mais inovadoras, competitivas, atraentes e resilientes, o que contribui para melhorar a vida de seus habitantes.

A cidade a ser protegida conta com alguns elementos fundamentais: um ecossistema urbano inserido em uma região, um conjunto que engloba infraestrutura, sistemas, plataformas e redes e uma população que interage, exerce seus direitos e busca a satisfação de suas necessidades. (Enerlis et al., 2012)

Essas cidades têm um novo ambiente, o ciberespaço, ou espaço digital, que é "um ambiente complexo composto por interações entre pessoas, programas de *software* e serviços na Internet por meio de dispositivos tecnológicos e redes conectadas a ela, que não existem na forma física" (ISO, 2012).

Figura 1.1.

O espaço digital como um ambiente complexo

Fonte: Elaboração própria (2021).

1.1
O que é cibersegurança?

A cibersegurança enfrenta os riscos inerentes à prestação de serviços no espaço digital. A União Internacional de Telecomunicações (UIT, 2018) propõe a seguinte definição de cibersegurança:

"Conjunto de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, métodos de gestão de riscos, ações, capacitação, melhores práticas, seguros e tecnologias que podem ser usados para proteger os ativos da organização e os usuários no ambiente cibernético."

"Os ativos da organização e dos usuários são os dispositivos de computação conectados, o pessoal, os serviços/aplicativos, os sistemas de comunicação, as comunicações multimídia e todas as informações transmitidas e/ou armazenadas no ambiente digital."


Arlington Research

"A cibersegurança garante a aplicação e manutenção das propriedades de segurança dos ativos e usuários da organização contra os respectivos riscos de segurança no ambiente cibernético."

O termo "cibersegurança" abrange todas as dimensões da segurança digital (OCDE, 2015): **1) a tecnologia,** quando incide no funcionamento do ambiente digital (muitas vezes chamada pelos especialistas de "segurança da informação", "segurança de TI" ou "segurança da rede"); **2) a aplicação da lei** ou aspectos jurídicos (por exemplo, crimes cibernéticos); **3) a segurança nacional** e a estabilidade internacional, inclusive aspectos como o papel das TICs na inteligência, prevenção de conflitos, guerra, defesa cibernética, etc., e **4) a dimensão econômica e social**, que compreende a criação de riqueza, inovação, crescimento, competitividade e emprego em todos os setores econômicos, liberdades individuais, saúde, educação, cultura, participação democrática, ciência, lazer e outras dimensões do bem-estar em que o ambiente digital promove o progresso.

Em uma cidade inteligente, a cibersegurança é a capacidade das autoridades, cidadãos e empresas de minimizar os riscos ou ameaças cibernéticas aos quais estão expostos quando realizam suas atividades ou desempenham suas funções no espaço digital.

A finalidade da cibersegurança é a proteção dos ativos digitais do ecossistema urbano e, para tanto, devem ser identificados os seguintes elementos:

1. **Governança**, políticas e diretrizes.
2. **Atores** e usuários.
3. **Ambiente**.
4. **Colaboração** e interação com o ambiente.
5. **Ferramentas** e instrumentos tecnológicos usados e que dão apoio à prestação dos serviços.
6. **As metodologias** aplicadas, boas práticas de gestão de riscos e gerenciamento de incidentes.
7. **Capacitação** e treinamento permanentes.

É possível distinguir dois tipos de ativos relacionados à segurança da informação (ISO, 2018): os ativos principais (processos e atividades de negócios e informações) e os ativos de apoio (aos quais os ativos principais estão condicionados) de todos os tipos: *hardware*, *software*, rede, equipe, site (portais virtuais ou infraestrutura física), estrutura organizacional.

1.2
Ecossistema de uma cidade cibersegura

O ecossistema da cidade que conta com cibersegurança é composto por:

i) cidadãos como beneficiários dos serviços;

ii) plataformas e redes de comunicação que permitem a distribuição da informação;

iii) infraestrutura tecnológica e sistemas de apoio à oferta dos serviços digitais oferecidos e as atividades das cidades e municípios;

iv) dispositivos conectados, aplicativos, dados e informações que transmitem;

v) um ecossistema urbano por meio do qual os serviços públicos são prestados; e

vi) capacidade de cibersegurança para a proteção de seus ativos, ou seja, uma instância que abriga todos esses elementos.

Infraestrutura tecnológica, fornecimento de energia, proteção de recursos, prestação de serviços e acesso a um bom governo são alguns dos princípios que as cidades e municipalidades procuram oferecer de forma eficiente por meio do uso de TICs. Esse uso pela cidade deve ser entendido de forma abrangente, de tal modo que as garantias de cibersegurança cubram cada uma das frentes em que os criminosos digitais tentarão explorar vulnerabilidades para atingir seus objetivos.

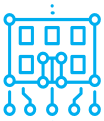
Figura 1.2.

Exemplos de elementos a serem protegidos

Infraestrutura de tecnologias:
Redes Wi-Fi, roteadores, dispositivos de conexão de rede, infraestrutura de tecnologias da informação, etc.

Dados e informações:
Dados de segurança, impostos, mobilidade, ambiente, cidadãos, etc.

Sensores e dispositivos:
Câmeras de vigilância, telefones celulares, sensores de iluminação, sensores de ambiente, de mobilidade, etc.



Sistemas e App:
Sistemas financeiros, de controle e gestão, aplicativos de serviços de saúde, mobilidade, etc.

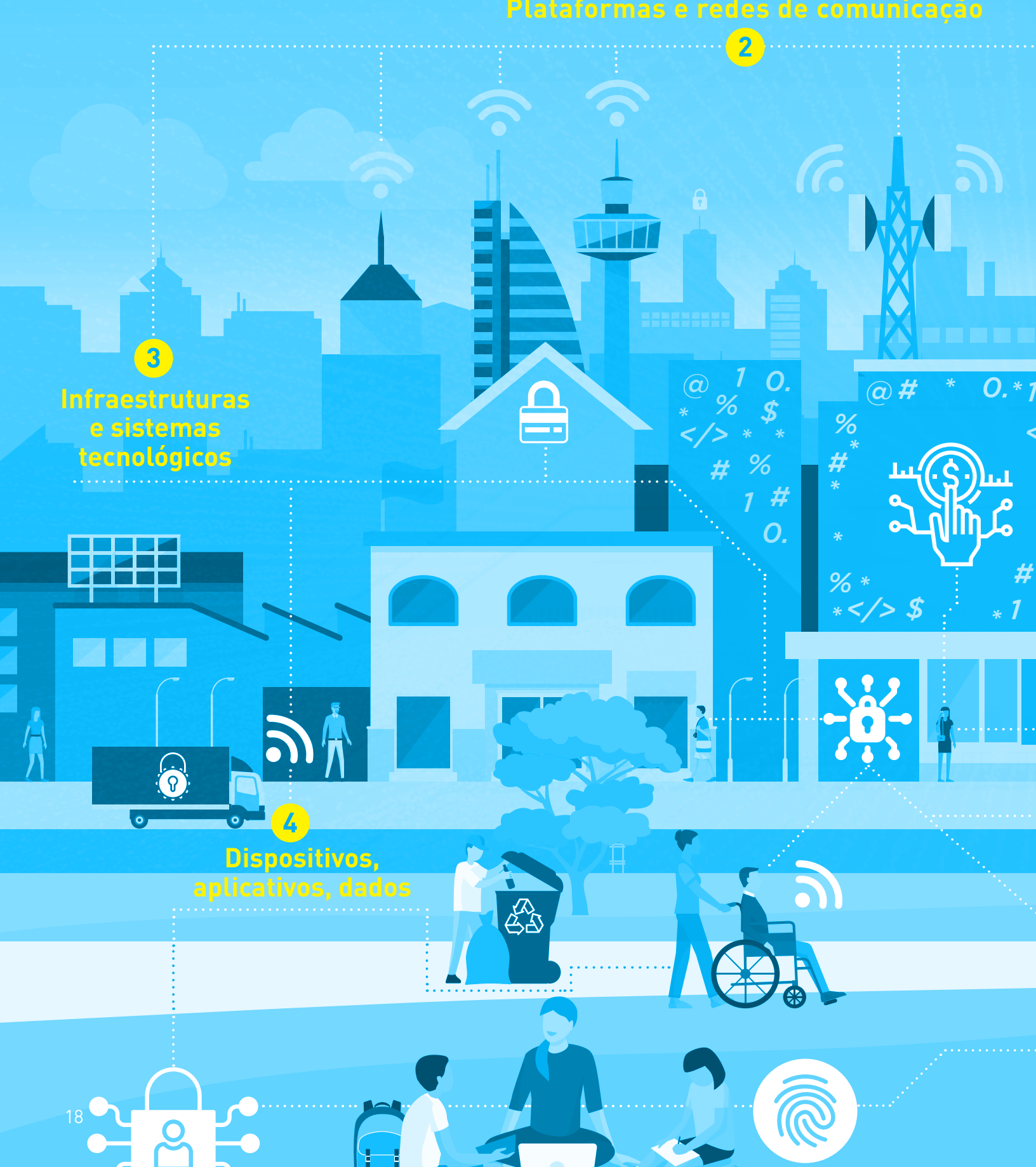
Fonte: Elaboração própria (2021).

Martin Adams

Figura 1.3.

Ecosistema da cidade com cibersegurança

Fonte: Elaboração própria (2021).




População
1
Capacidade de cibersegurança
6
Ecossistema urbano
5

1.3
Níveis estratégico, tático e operacional de gestão da cibersegurança

A cibersegurança deve ser gerida desde o nível estratégico dos dirigentes da cidade, passando pelo nível tático de gestão dos secretários e chegando ao nível operacional dos técnicos em cibersegurança e de TIC.

Figura 1.4.

Níveis de gestão da cibersegurança

Estratégico

Responsável pela direção geral, definir a visão, alocar recursos, assumir responsabilidades e priorizar os objetivos de segurança cibernética da cidade, bem como empoderar as equipes técnicas para liderar e orientar as estratégias visando a consecução dos objetivos. Aprova a governança, normas, diretrizes, políticas e gestão dos recursos demandados por elas. Exige o cumprimento de todas as funções.

Tático

Responsável pela execução das normas. Assegura que as equipes cumpram as normas, diretrizes e políticas, geralmente por meio da definição de planos, programas e projetos alinhados com as políticas priorizadas. Trata-se de um nível de planejamento específico que aprofunda o detalhamento de cada um dos setores (governo, mobilidade, saúde, etc.).

Operacional (técnico)

Propõe as normas, diretrizes, políticas, padrões e recursos necessários para atingir os objetivos. Formula e executa as estratégias, monitora e supervisiona a execução. Entre outras atribuições, propõe diretrizes técnicas e de capacitação e os procedimentos de gestão, identificação, proteção, detecção, reação e recuperação de incidentes (esta atividade pode ser realizada por pessoal diretamente vinculado à cidade ou município, ou por terceirizados).

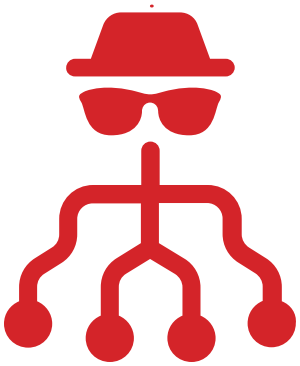
Fonte: Elaboração própria (2021).

1.4

Ataques cibernéticos contra as cidades

Quando um risco se concretiza, ocorre um ataque digital que danifica ou ameaça, entre outros, dados, informações, infraestrutura e, em termos gerais, qualquer um dos ativos indicados no item 1.1 deste guia.

Os principais atores e motivos para a realização de um ataque cibernético estão listados abaixo; são apresentados também os principais tipos de ataques e vulnerabilidades e, evidentemente, os efeitos observados quando uma cidade ou município é confrontado com um ataque cibernético.



1.4.1

Principais atores e motivos para realizar um ataque cibernético

São várias as motivações que influenciam a concretização de um ataque: superação de um desafio pessoal, obtenção de informações comerciais ou estatais privilegiadas, consecução de um objetivo político ou obtenção de um valor econômico. Esses motivos não são mutuamente excludentes; pelo contrário, em um ataque digital podem coexistir, por exemplo, uma atividade criminosa de espionagem industrial ou política.

Qualquer um desses motivos serve como base para colocar os municípios em risco. Esses podem ser motivos de um ou mais atores, como veremos a seguir.

Figura 1.5.

Motivos para realizar um ataque cibernético contra uma cidade

Pessoal

O criminoso deseja satisfazer um desejo, uma necessidade ou qualquer outra questão relacionada a si próprio. A superação pessoal, superação de um desafio, curiosidade, vingança, satisfação pessoal, entre outros, podem constituir um motivo para cometer um ataque cibernético.

Empresarial

A colocar as informações em perigo, obter segredos empresariais, conhecer a atividade empresarial, a infraestrutura de prestação dos serviços e, de forma geral, os bens ou serviços oferecidos, podem ser motivos para a concretização de um ataque cibernético.

Econômico

A realização de um ataque pode objetivar uma retaliação, compensação, benefício ou ganho para o autor do ataque ou para um terceiro.

Criminoso

A motivação criminosa pode estar ligada a dois propósitos. Por um lado, causar dano, lesionar ou colocar em perigo o patrimônio jurídico da vítima; por outro, a obtenção de um benefício para o autor do crime ou para um terceiro.

Político

A motivação criminosa pode estar associada à mudança do regime político vigente, queda de um setor democrático, direcionamento para a tomada de uma decisão cidadã, ameaça ou desestabilização da soberania, governo, território ou população de uma nação.

Outros motivos

Existem outras motivações. Além disso, pode haver motivos que se complementam entre si. Um exemplo pode ser a prática de uma atividade criminosa por vingança que, ao mesmo tempo, tenha um motivo comercial ou econômico.

Fonte: Elaboração própria (2021).

Em todo ataque cibernético, há um conjunto de atores, vítimas e perpetradores. O papel que cada ator desempenha é detalhado na Figura 1.6.

Figura 1.6.

Principais atores dos ataques cibernéticos

Ativos

Aqueles que, realizam direta ou indiretamente o ataque cibernético para diversos fins:

- Ciber**criminosos**
- Ciber**espiões**
- Ciber**terroristas**
- Ciber**ativistas**

Passivos

As vítimas do ataque cibernético:

- **Cidadãos**
- **Empresas** ou entidades privadas
- **Estados** ou qualquer autoridade pública (por exemplo, municípios)

Qualquer que seja o tipo de ator (ativo ou passivo)

Públicos | **Privados** | **Nacionais**

Estrangeiros | **Individuais** | **Coletivos**

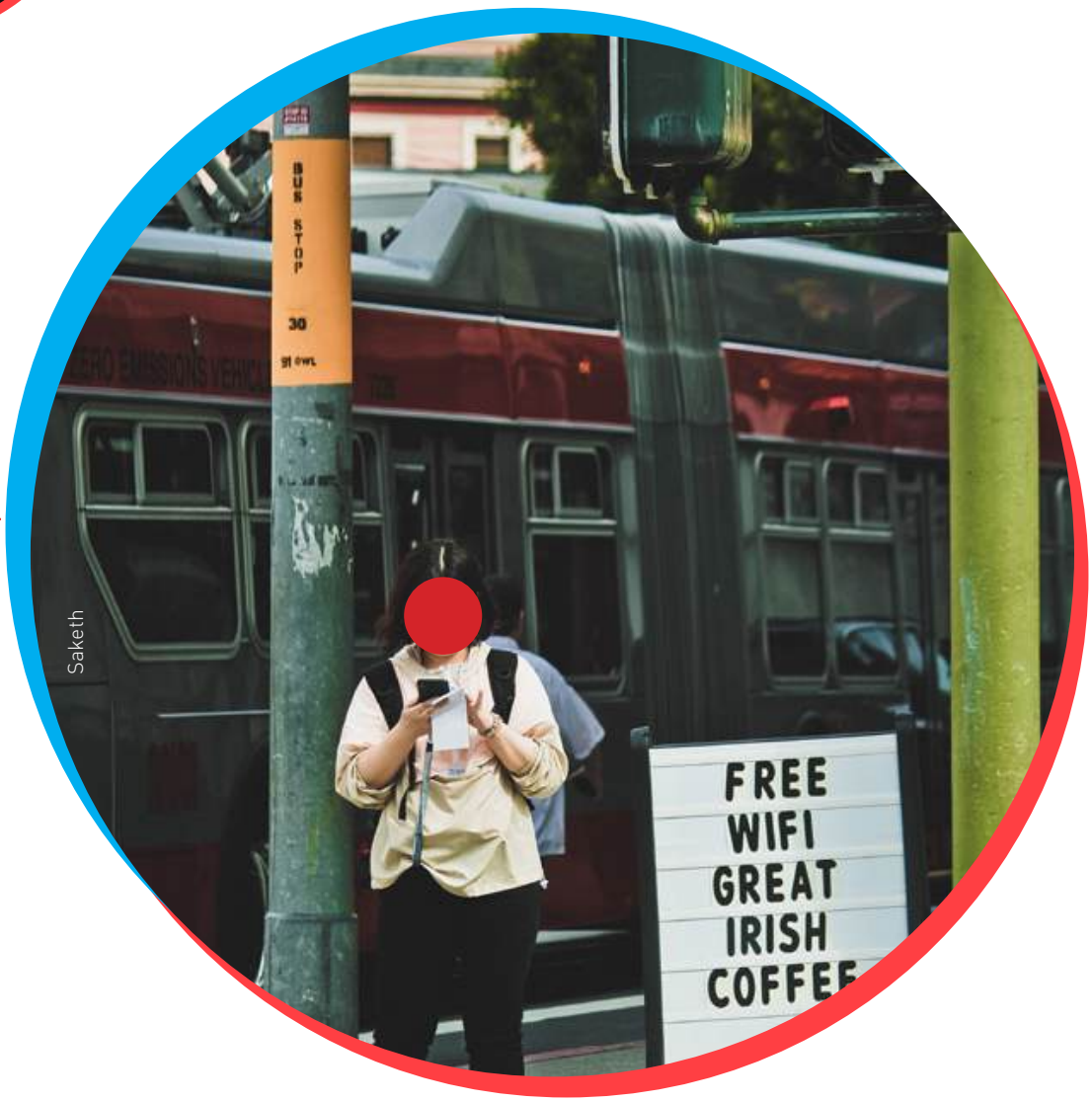
Fonte: Elaboração própria (2021).

Com base em cada um dos papéis desempenhados pelos diversos atores, é preciso compreender os tipos de ameaças a que o ecossistema urbano como um todo pode estar sujeito.

1.4.2
Principais tipos de ataques e vulnerabilidades

Os alvos de um ataque cibernético podem ser informações, *hardware*, *software*, serviços oferecidos, redes e conexões, recursos humanos, infraestrutura cibernética crítica e, em geral, qualquer bem ou serviço municipal que utilize TICs. Os ataques mais frequentes estão relacionados ao uso de engenharia social, programas mal-intencionados, força bruta para obter acesso e ataques a conexões e infraestrutura. Tais ações visam, entre outros objetivos, atentar contra a privacidade, integridade ou disponibilidade dos sistemas de informação e, de forma geral, driblar medidas de segurança.


Arian Darvishi



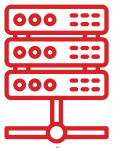
Saketh

As autoridades urbanas e municipais devem conhecer as técnicas mais frequentes (também chamadas de técnicas de hacking) e os principais tipos de ameaças. A Figura 1.7 resume algumas delas.

Figura 1.7.

Tipos de ameaças e ataques cibernéticos

Ransomware *ou extorsão digital*
Atividade por meio da qual se assume o controle do dispositivo e se criptografa as informações; em alguns casos, estas são extraídas sob ameaça de publicação. É exigido o pagamento de um resgate para recuperação do controle e das informações.



Ataque de negação de serviço distribuído (DDoS)
Cometido contra um servidor ou rede a partir de vários computadores simultaneamente, com redes zumbis, para que pare de funcionar por não conseguir processar tantas solicitações.

Clonagem de rede (Wi-Fi falso)
Criação de uma rede Wi-Fi a partir de outra legítima e segura, com nome igual ou muito semelhante ao da original, com o intuito de furtar os dados de quem se conectar a ela.

Phishing *ou isca digital*
Envio de mensagens com o uso de uma identidade que aparenta ser legítima com o intuito de intrusão e ataque.

Spoofing / *mascaramento/falsificação de origem de e-mail*
Uso do endereço de e-mail de uma pessoa ou entidade de confiança para obter informações pessoais por meios fraudulentos.

Dispositivos zumbis/botnets
Vários dispositivos diferentes infectados ao mesmo tempo, controlados por criminosos digitais.

Engenharia social
Conjunto de técnicas destinadas a manipular psicologicamente os usuários para que comentam uma ação comprometedora, como, por exemplo, pela revelação de informações pessoais ou navegação em páginas mal-intencionadas, o que permite assumir o controle dos dispositivos.

Injeção de SQL
Ataque a um serviço da web baseado neste tipo de linguagem, comprometendo a base de dados por meio de linhas de código mal-intencionado e explorando vulnerabilidades em sua programação.

Spam *ou e-mails indesejados*
Envio não solicitado de grandes quantidades de mensagens ou materiais publicitários pela Internet.

Cavalos de Troia
Vírus para controlar um computador, roubar dados, introduzir mais *software* mal-intencionado no computador e se propagar para outros dispositivos.

Anúncios mal-intencionados
Visam a coleta de informações sobre a atividade do usuário e, assim, a exibição de anúncios direcionados. Sua instalação pode causar queda no desempenho e mau funcionamento do dispositivo.

"Man in the middle"
Conhecido como o ataque do intermediário. Aqui, o intermediário mal-intencionado se situa entre dois ativos que estão se comunicando e intercepta a comunicação; dessa forma, obtém acesso para ler ou manipular os dados, mensagens, credenciais ou transferências nos dois sentidos.

Fonte: Elaboração própria (2021).

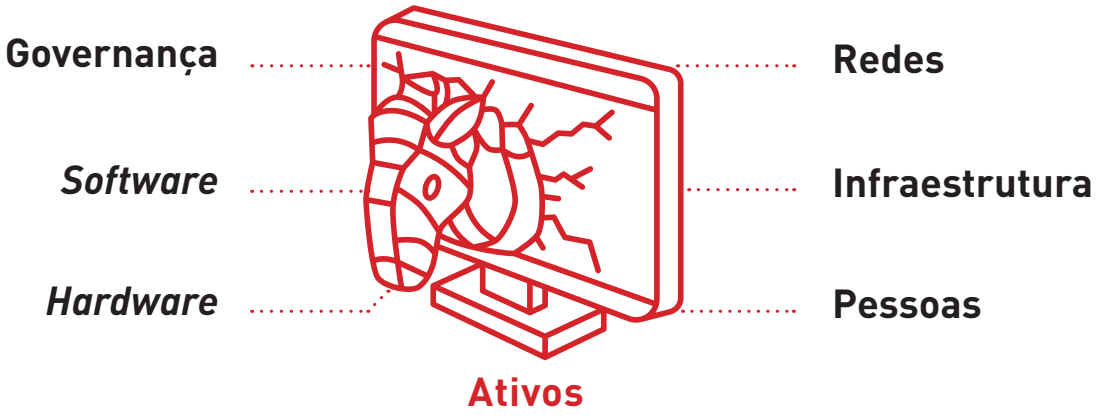
Existem também outras técnicas e métodos de ataque, como o analisador de dados, aplicativos mal-intencionados, ataques de *cookies*, envenenamento do cache de DNS, mascaramento de IP, varredura de portas, antivírus falso, *worms*, *backdoors*, registrador de teclas, *spyware*, mascaramento de site, sequestro de informações confidenciais, ataques ciberfísicos e mineração de criptografia, entre outros. Todas essas ações podem ser combinadas entre si e os resultados podem ser devastadores.

Os ataques cibernéticos ocorrem porque existem vulnerabilidades, ou seja, falhas nos ativos (*software, hardware,* redes, infraestrutura), interação entre os ativos ou a governança. Além disso, o **fator humano** constitui um dos principais pontos fracos que os cibercriminosos aproveitam para alcançar seus objetivos. Esses pontos fracos podem ter origem dentro ou fora das organizações, por meio de cadeias de suprimentos e outros terceiros (clientes, autoridades de controle, etc.).

Por isso, é imprescindível a implantação de controles em caráter permanente, a identificação de vulnerabilidades, capacitação constante, colaboração entre as partes interessadas e gestão adequada dos riscos e incidentes, cada um dos quais passa a ser a principal atividade para a proteção dos ativos da organização.

Figura 1.8.

Origem das principais falhas e vulnerabilidades



Fonte: Elaboração própria (2021).

Entre outros, os criminosos digitais se aproveitam das falhas e vulnerabilidades existentes nas cidades, vinculadas às seguintes falhas:

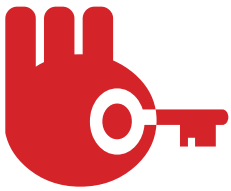
1. **Inexistência de uma estratégia de cibersegurança abrangente.**
2. **Falta de governança, normas, diretrizes e políticas de cibersegurança.**
3. **Falta de integração completa da cadeia de suprimentos e de terceiros que se relacionam com a cidade no processo de cibersegurança.**
4. **Inexistência de uma política de proteção de dados.**
5. **Ausência de uma gestão adequada das vulnerabilidades, riscos e incidentes.**
6. **Falta de atualização do *software* e *hardware* disponível para a prestação dos serviços da cidade.**
7. **Falhas no *software* e *hardware* existentes.**
8. **Falta de capacitação e treinamento do pessoal e demais partes envolvidas (terceiros, usuários).**
9. **Falta de recursos financeiros para desenvolver a estratégia de cibersegurança da cidade.**
10. **Falta de cooperação e colaboração entre as diversas autoridades e o setor privado.**
11. **Ausência de capacidades (recursos humanos, ferramentas, tecnologias).**
12. **Falta de compreensão do ambiente digital.**
13. **Aplicação inexistente ou errônea de controles técnicos.**

Bermix

1.4.3

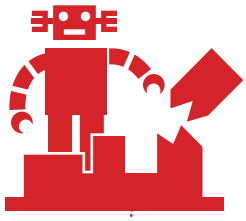
Possíveis consequências de um ataque cibernético à cidade

Os riscos concretizados por meio dos ataques geram consequências como as seguintes:



- **Interrupção de serviços essenciais** da cidade, como energia, abastecimento/tratamento de água, mobilidade, saúde, controle de tráfego, etc.
- **Redução da produtividade** dos trabalhadores.
- **Suspensão da arrecadação** de impostos municipais.
- **Impossibilidade de prestação** de serviços ao cidadão, como a realização de procedimentos ou emissão de autorizações, entre outros.

- **Danos reputacionais** ao governo municipal e desconfiança.
- **Transgressão das leis** de privacidade e confidencialidade de dados, o que pode dar margem a investigações e penalidades.
- **Perda dos investimentos** realizados para a prestação de serviços.
- **Desestabilização política, econômica ou social.**
- **Impactos na integridade, disponibilidade, confidencialidade e autenticidade dos dados.**



1.5

Ataques cibernéticos que paralisaram cidades

Giacomo Carra

Christian Wediger

De acordo com a taxonomia de danos digitais proposta por Agrafiotis (2018), estes compreendem cinco categorias gerais: i) dano físico ou digital, ii) dano econômico, iii) dano psicológico, iv) dano reputacional e v) dano social. Esses danos podem estar interligados e, dependendo do ataque, pode haver propagação em maior ou menor grau. Centenas de milhares de ataques cibernéticos ocorrem diariamente, muitos deles tendo como alvo cidades e outras infraestruturas críticas.[2] Felizmente, a grande maioria é irrelevante, precisamente graças à cibersegurança. Desde 2003, ocorreram quase 1.000 ataques digitais, que custaram mais de US$ 1 milhão (CSIS, 2021) cada um, e mais de 500 sequestros de dados relevantes em 2020 e 2021.[3]

Apesar dos anos que se passaram, o **ataque digital contra a Estônia, em abril de 2007, foi um ponto de inflexão para as autoridades públicas, e as cidades começaram a levar a cibersegurança a sério.** Após a polêmica remoção de uma estátua, houve uma enxurrada de solicitações de acesso (DDoS) que obstruiu a rede de Internet do país e impediu o acesso a servidores, bancos, jornais e diversos serviços eletrônicos do governo. O ataque afetou mais de um milhão de computadores que, por ter acessado um e-mail ou página, baixaram um *software* mal-intencionado que os transformou em zumbis controlados à distância para se conectar ao mesmo ponto para derrubá-lo. O lado positivo foi que a **situação chegou até a Organização do Tratado do Atlântico Norte (OTAN), o que abriu caminho para a cibersegurança na União Europeia e em organismos internacionais.** Além disso, desde então o governo da Estônia entendeu a importância de uma estratégia de cibersegurança, a necessidade de promoção pública e de colaboração entre o Estado, o setor privado e a esfera acadêmica. **A Estônia se tornou um dos países digitalmente mais avançados do mundo,** em grande parte devido à reação a esse ataque. Nesse caso, os danos foram sociais, digitais e econômicos.

2. Ver: https://www.sicherheitstacho.eu/start/main, https://cybermap.kaspersky.com/es, https://www.fireeye.com/cyber-map/threat-map.html, https://horizon.netscout.com.

3. Ver https://cloudian.com/ransomware-attack-list-and-alerts.


Bermix

Entre os ataques cibernéticos de destaque dos últimos anos, cabe lembrar que seus alvos têm sido a polícia e os serviços de emergência ou de transportes das cidades. Em abril de 2021, os ataques digitais extraíram mais de 250 GB de informações altamente confidenciais do Departamento de Polícia de **Washington, D.C.** Como prova disso, os criminosos divulgaram parte das informações, exigiram dinheiro e ameaçaram "entrar em contato com quadrilhas para expurgar os informantes" (da polícia). Essa ação se caracterizou como um caso de extorsão digital. Trata-se de um ataque que segue a linha já marcada em junho de 2017, quando *hackers* conseguiram acionar as sirenes de alerta de tempestades, desastres, etc. da população norte-americana de **Dallas,** no Texas, o que provocou o colapso das linhas de emergência. Em janeiro de 2017, criminosos assumiram, durante quatro dias, o controle das câmeras de segurança do Departamento de Polícia Metropolitana do Distrito de Columbia (MPDC). Em novembro de 2017, o Sistema Regional de Trânsito de Sacramento, nos Estados Unidos, foi alvo de um ataque cibernético cujo resultado final foi a perda de informações de programas e dados necessários para a saída de ônibus e o planejamento de rotas.


Nataniael Melchor

O sistema de saúde também tem sido um alvo importante, o que tem sido oneroso. Com efeito, em janeiro de 2020, um ataque cibernético ao Hospital Universitário de Torrejón, em **Madrid**, na Espanha, danificou vários dos sistemas de TI (danos digitais). Essa linha havia sido traçada há alguns anos e tem como precedente de destaque o mês de maio de 2017, quando a rede hospitalar de Londres sofreu um sequestro de dados digitais (*ransomware*) que afetou hospitais, postos de saúde e pacientes, entre outros. A rede de ambulâncias foi prejudicada, o pessoal médico não conseguia acessar os prontuários dos pacientes e a vida dos cidadãos foi colocada em perigo; milhares de consultas foram canceladas e pacientes de emergência foram remanejados. Estima-se que o custo tenha sido de US$ 130 milhões (R$ 715 milhões).[4]


Brad Huchteman

Atlanta, Estados Unidos: uma cidade em colapso e um governo exonerado por não investir em cibersegurança em tempo hábil. Em março de 2018, usando força bruta, criminosos conseguiram descobrir as senhas em Atlanta. Isso afetou muitos serviços e programas da cidade durante semanas, inclusive estacionamentos e serviços judiciais. Os servidores municipais se viram obrigados a preencher formulários manualmente. Cabe destacar que, antes do ataque, o governo de Atlanta havia sido criticado pelos investimentos baixos e pelas falhas na cibersegurança. Posteriormente, a falta de investimento em tempo hábil acarretou um enorme custo político e econômico. Assim, a situação levou à demissão de dezenas de servidores e de toda a equipe de governo. Atlanta teve de investir US$ 2,7 milhões para se recuperar.

4. Ver https://www.acronis.com/en-us/articles/nhs-cyber-attack.


Calin Lloyd

O sequestro digital da **cidade de Baltimore (Maryland, Estados Unidos)** foi certamente um pesadelo. Em maio de 2019, um ataque de sequestro de dados (*ransomware*) bloqueou computadores, sistemas e e-mails, entre outros ativos da prefeitura. O resgate pedido ao governo foi de 13 bitcoins (aproximadamente US$ 76.280), mas o prefeito se recusou a pagar.[5] Estima-se que essa decisão tenha gerado um custo de US$ 18,2 milhões. A cidade passou três semanas em situação anormal e demorou meses para conseguir se recuperar.

Colonial Pipeline

Em agosto de 2021, dados da **Prefeitura de Santa Fé de Antioquia, na Colômbia**, foram sequestrados e usados para fins de extorsão. Em consequência disso, os cidadãos não puderam realizar procedimentos virtuais e foi decidido congelar as contas municipais. Do mesmo modo, em março de 2021, o **Serviço Público de Emprego Estatal (SEPE) da Espanha** foi alvo de um ataque do *ransomware* Ryuk, que dificultou e atrasou em três semanas a gestão dos pagamentos de seguro-desemprego. Nesse caso, foi destacado o fato de os sistemas de TI não estarem suficientemente atualizados, o que possibilitou o ataque. Em maio de 2021, o **governo dos Estados Unidos** decretou estado de emergência regional devido a um ataque de *ransomware* aos sistemas do **Colonial Pipeline**, a maior rede de oleodutos do país. O ataque conseguiu desconectar a infraestrutura tecnológica do oleoduto, que se estende por quase 9.000 quilômetros entre o Texas e New Jersey e conduz 45% do diesel, gasolina e combustível consumidos pelos aviões da costa leste do país. Foi um sequestro do tipo *ransomware*, onde foi exigido o pagamento de resgate.

Em dezembro de 2019, o governo da **província de San Luis, na Argentina**, teve de declarar estado de emergência por 90 dias: seu sistema de arquivos foi sequestrado com o pedido de um resgate. Ao que parece, a cidade não pagou e conseguiu recuperar as informações até dezembro de 2018, mas houve problemas significativos para descriptografar os 350 GB de dados correspondentes a todo o ano de 2019. Já o **Ministério da Economia do México** teve de suspender os prazos administrativos depois que arquivos e e-mails foram afetados após um ataque em fevereiro de 2020.

5. Disponível em https://twitter.com/mayorbcyoung/status/1136377418325864448.

Em junho de 2021, a **Universidad del Bosque, da cidade de Bogotá,** informou a comunidade acadêmica que havia sido vítima de um ataque à cibersegurança, no qual alguns de seus sistemas internos foram comprometidos. Supõe-se que esse ataque se deu por meio de uma negação de serviços distribuída e resultou no bloqueio das atividades administrativas e acadêmicas por vários dias.

Uma história com final feliz graças à previsão. Em junho de 2021, a rede metroviária de Nova York sofreu um ataque cibernético. A Metropolitan Transit Authority (MTA) contava com uma estratégia de cibersegurança robusta, o que lhe permitiu conter o ataque e manter a prestação de seus serviços. Aparentemente, o planejamento e as múltiplas camadas adotadas pela MTA funcionaram conforme planejado. Além disso, nos últimos meses, havia sido desenvolvida uma sensibilidade especial, bem como elementos de previsão, após vários ataques contra infraestruturas críticas nos Estados Unidos.

Com a COVID-19, surgiram novas formas de ataques digitais. A engenharia social, a extrema necessidade de suprimentos essenciais e informações relacionadas à COVID-19 começaram a ser usadas como iscas para a obtenção de dados, golpes e *phishing*, e houve o sequestro de computadores por meio de *malware*, anexos mal-intencionados e roubo de identidade. Também houve ataques de *ransomware* e DDoS contra hospitais e postos de saúde com carência de pessoal. Da mesma forma, a vulnerabilidade do *home office* foi explorada para furtar dados, obter lucro ou causar disfunções (Interpol, 2020). Assim, por exemplo, em março de 2020, na **Costa Rica**, um aplicativo de *ransomware* chamado COVIDLock se espalhou por todo o país e afetou também o setor público. Teoricamente, o aplicativo oferecia mapas interativos da disseminação do vírus, e aproveitava o interesse dos usuários para sequestrar os dispositivos e exigir pagamento de resgate em *bitcoins* (prejuízos econômicos e sociais).

1.6

A maturidade das cidades inteligentes em cibersegurança

Segundo conclusão do Instituto Nacional de Normas e Tecnologia (NIST)[6] (NIST, 2019), as cidades e comunidades inteligentes não são sustentáveis ou verdadeiramente inteligentes se não identificarem, implantarem e mantiverem processos e medidas de gestão de riscos de cibersegurança e privacidade de forma proativa e adaptativa. Isso também gera confiança e facilita a participação na cidade inteligente.

Em sua Recomendação 7, a Agência Europeia para a Segurança das Redes e da Informação (ENISA) (ENISA, 2015) aponta que as cidades inteligentes e os organismos de padronização devem integrar a cibersegurança como quesito de maturidade urbana. Assim, as cidades mais maduras poderão compartilhar suas medidas de segurança como exemplo, e as menos maduras, além do aprendizado, terão incentivos para melhorar.

No entanto, não há conscientização suficiente. Os rankings internacionais de maturidade digital das cidades mais destacados não contemplam a cibersegurança: IMD-SUTD Smart City Index (SCI),[7] Top 50 Smart City Government Rankings (smartcitygovt),[8] Smart City Winners, IESE's Top 10 By Dimension,[9] JUNIPER Research 2019-2023,[10] etc.

Melhoria da situação. Por um lado, o BID começou a integrar segurança e privacidade em seus cinco níveis destinados a medir o grau de maturidade da *smart city* (Townsend e Zambrano-Barragán, 2019: 19 e ss.). Por outro lado, segurança e privacidade constituem uma das quatro dimensões do diagnóstico de maturidade de Big Data para o desenvolvimento urbano (Biderman et al., 2021). Recentemente, o roteiro para as "cidades pioneiras" do G-20 passou a incorporar a segurança e a privacidade como elementos essenciais (Aliança Global de Cidades Inteligentes do G-20, 2021). E no Japão (MIAC, 2020), privacidade e segurança também são elementos básicos.

6. O Instituto Nacional de Normas e Tecnologia (NIST) faz parte do Departamento de Comércio dos EUA. O Marco de Cibersegurança co NIST ajuda empresas de todos os portes a entender melhor seus riscos de cibersegurança, gerenciar e reduzir seus riscos e proteger suas redes e dados.

7. Ver https://www.imd.org/smart-city-observatory/smart-city-index.

8. Ver https://www.smartcitygovt.com.

9. Ver https://smartcity.press/top-10-smart-cities-of-2020.

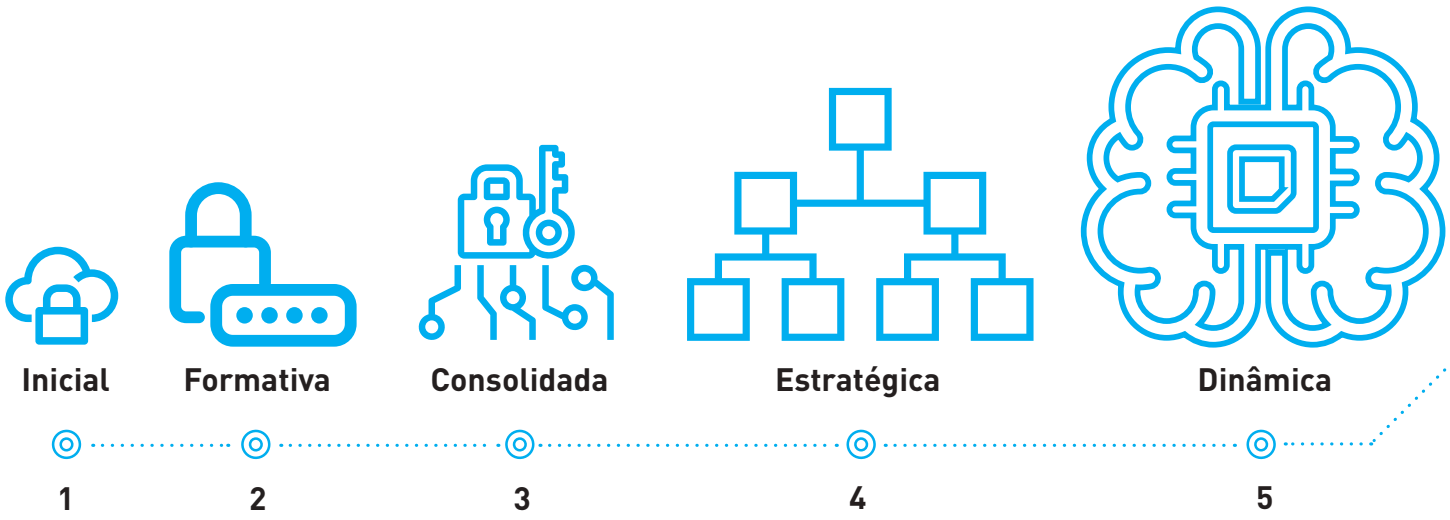
10. Ver https://www.juniperresearch.com/researchstore/key-vertical-markets/smart-cities-research-report/subscription/leading-platforms-segment-analysis-forecasts.

A Aliança Global de Cidades Inteligentes do G-20 sobre Governança de Tecnologia, que reúne governos municipais, regionais e nacionais, parceiros do setor privado e da sociedade civil, foi criada em 2019 com o intuito de coletar e analisar políticas para o sucesso de cidades éticas e inteligentes. Já existe uma política modelo de governança (Aliança Global de Cidades Inteligentes do G-20, 2020) e um roteiro (FEM, 2021), no qual a cibersegurança foi incorporada como elemento multidisciplinar.

Na ALC, somente a partir de 2016 houve um maior interesse na criação de segurança para os países no ambiente digital. Por meio de uma colaboração do BID e da OEA (BID e OEA, 2020), foi estabelecido na América Latina e no Caribe, o Modelo de Maturidade da Capacidade de Cibersegurança para as Nações (CMM, na sigla em inglês). Este modelo, elaborado pelo Centro Global de Capacidade em Segurança Cibernética da Universidade de Oxford, avalia o nível de maturidade das capacidades de cibersegurança de um país em cinco estágios: 1) Inicial; 2) Formativa; 3) Consolidada; 4) Estratégica e 5) Dinâmica.

Figura 1.9.

Os cinco estágios da maturidade da capacidade de cibersegurança

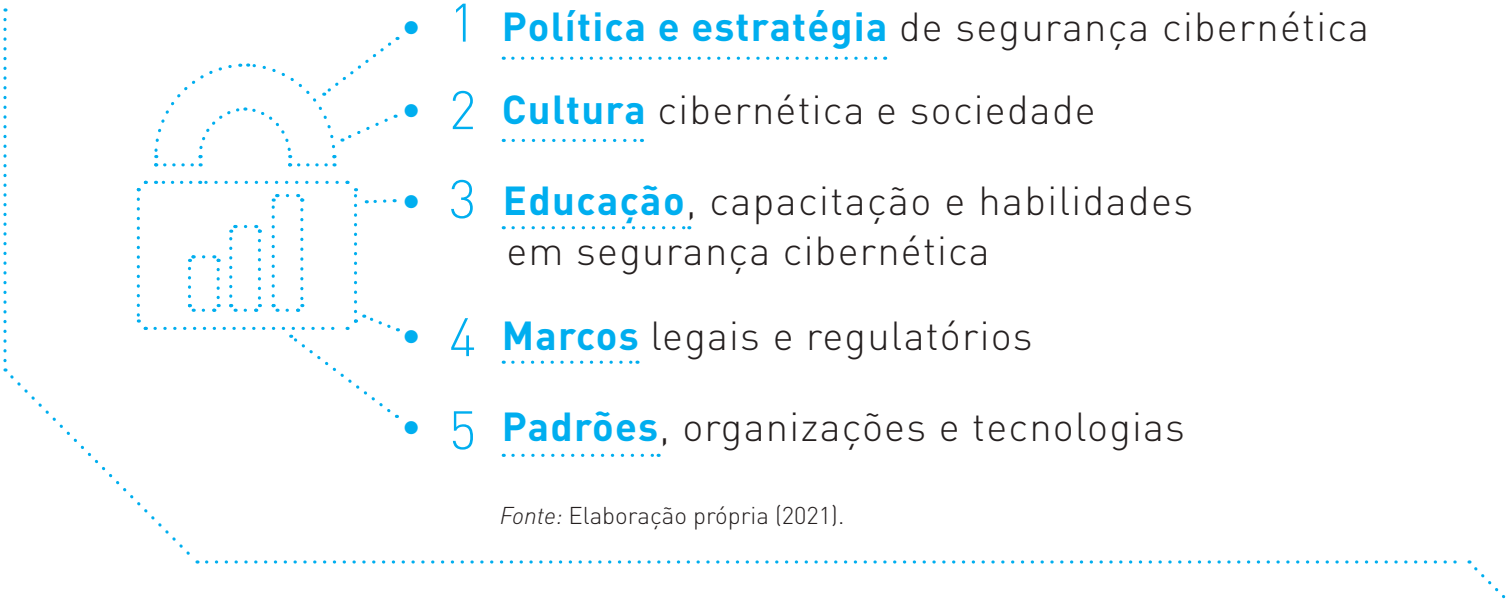


Fonte: BID e OEA (2020: 42).

Por sua vez, a avaliação dos níveis de maturidade é dividida em cinco dimensões: 1) Política e estratégia de cibersegurança; 2) Cultura cibernética e sociedade; 3) Capacitação, treinamento e competências em cibersegurança; 4) Marcos legais e regulatórios; e 5) Padrões, organizações e tecnologias. Elas são subdivididas em um conjunto de fatores que descrevem e definem o que significa dispor de capacidade de cibersegurança em cada fator e indicam como melhorar a maturidade. Os indicadores e o modelo também são úteis como referência para as cidades.

Figura 1.10.

As cinco dimensões do modelo de maturidade da capacidade de cibersegurança para as nações



Fonte: Elaboração própria (2021).

Entre as principais conclusões dos relatórios (2016, 2020), verifica-se um aumento significativo do interesse e sensibilização em cibersegurança, bem como um aumento considerável da maturidade nessa área, o que inclui a ampliação da capacidade dos órgãos de governo e a elaboração de estratégias e legislações nacionais. Os países da região trilharam o caminho para a transformação digital com cibersegurança, e o desafio é que as cidades sejam capazes de implantar muitos dos elementos apresentados nestes relatórios.

No processo de migração para uma *smart city* e no uso do conceito de *Big Data* urbano, é fundamental que sejam incorporadas capacidades que permitam um nível adequado de cibersegurança. Ademais, o cumprimento da função de cibersegurança deve ser definido como uma prioridade para que os serviços oferecidos na cidade sejam seguros.

Markus Spiske Iar

2 Recomendações e recursos para proteger as cidades dos ataques cibernéticos

Daniel Lloyd Blunk Fernández

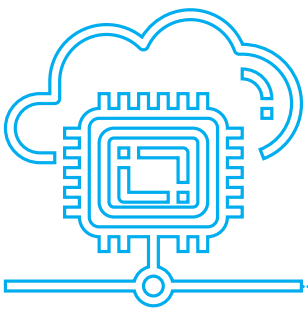
"A arquitetura e infraestrutura tecnológica de uma cidade são complexas; os atores envolvidos são muito variados, o que também ocorre com as informações e dados que devem ser protegidos."

2 Recomendações e recursos para proteger as cidades dos ataques cibernéticos

Os leitores deste guia já conhecem o conceito de cibersegurança e de ameaças cibernéticas que colocam as cidades em xeque no espaço digital. Para proteger as cidades dos ataques cibernéticos é necessário implementar ações proativas para fortalecer a cibersegurança. Há alguns anos, o BID publicou *Caminho para as smart cities* (Bouskela et al., 2016: 115). O que se propõe agora é um roteiro para a cibersegurança das cidades. A Figura 2.1 contém tal roteiro, com as recomendações, práticas e recursos necessários para proteger qualquer tipo de cidade com uma abordagem baseada na gestão de riscos.

Figura 2.1.

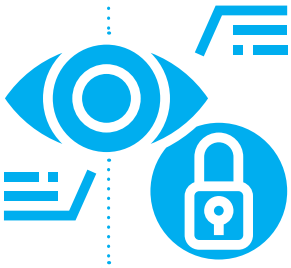
Roteiro para a cibersegurança urbana



1. **Identificar** os ativos e atores a serem protegidos
2. **Definir** a governança da segurança cibernética
3. **Institucionalizar** a segurança cibernética
4. **Integrar** a segurança dos dados confidenciais da cidade à dos dados pessoais
5. **Integrar** os provedores à segurança cibernética
6. **Formar**, comunicar e conscientizar acerca da segurança cibernética
7. **Dispor** de financiamento e seguros para segurança cibernética

Fonte: Elaboração própria (2021).


Daria Nepriakhina



A arquitetura e infraestrutura tecnológica de uma cidade é complexa; os **atores** envolvidos são muito variados, o que também ocorre com as **informações e dados** que devem ser protegidos. Por isso, o primeiro passo é a identificação de todos esses elementos (NIST, 2019), o que deve ficar basicamente a cargo do pessoal tático e tecnológico da cidade.

A partir do conhecimento da complexidade da cidade e dos temas a serem protegidos, o nível estratégico deve estabelecer uma **governança** que integre a gestão da cibersegurança, da cidade inteligente e dos dados. Como pressuposto, devem ser levados em consideração as leis e regulamentos de cumprimento obrigatório, para o quê o nível tático pode dar um apoio importantíssimo. Além disso, a partir dos perfis tecnológicos é preciso escolher entre os diversos esquemas de padronização e certificação de cibersegurança. Nesse sentido, recomenda-se que o nível estratégico estabeleça políticas e padrões comuns de segurança para a cidade, com atribuições claras e envolvimento das partes interessadas. A cibersegurança urbana também deve estar conectada às políticas nacionais. O estabelecimento de uma governança implica a **institucionalização** a cargo do nível estratégico. Deve ser designado um gestor da cibersegurança, com as atribuições específicas aqui descritas. Aqui são esboçadas também as melhores práticas para permitir aos níveis tático e tecnológico compartilhar informações de segurança.

É necessário proteger as informações e os dados. De forma geral, o nível tático identifica, segundo os parâmetros legais, se há dados confidenciais e pessoais que devam receber proteção especial, e o nível tecnológico implementa a proteção correspondente. As melhores práticas a este respeito incluem a anonimização (e pseudonimização) e a criptografia dos dados geridos pela cidade.

Da mesma forma, recomenda-se **integrar à cibersegurança a seleção, gestão e contratação de fornecedores e prestadores de serviços**, para o quê o pessoal de nível tático é essencial. Cabe também mencionar que, entre as recomendações e melhores práticas mais importantes, encontram-se **a cultura de cibersegurança, a conscientização e a capacitação** dos gestores e dos servidores municipais. Finalmente, é essencial contar com um orçamento para a cibersegurança e considerar a possibilidade de contratação de seguros. Isso requer uma dinâmica de nível estratégico, juntamente com o apoio tático.

Zhang Kaiyv

2.1
Identificar os ativos e atores a serem protegidos

Atualmente, a prestação de serviços e a gestão da infraestrutura urbana por meio das TICs é fundamental para a cidade. Entretanto, sua utilização implica a gestão dos riscos envolvidos. Como observado na seção anterior, muitas cidades têm sofrido a paralisação dos serviços devido a diversos ataques cibernéticos.

Inicialmente, **é preciso identificar o que será protegido, ou seja, os principais ativos (processos e atividades institucionais e dados críticos)** e os ativos de apoio a essas informações (***hardware*, *software*, rede, pessoal, estrutura organizacional**, etc.) que precisam ser protegidos, além de mensurar o possível impacto de um ataque cibernético.

É preciso ter consciência de todos os elementos inteligentes que dependem do espaço digital e não estão protegidos: sistemas industriais inteligentes (redes SCADA) como, por exemplo, sistemas de distribuição de eletricidade, de vigilância e de sensores de variáveis ambientais, que dependem da Internet das Coisas (IoT, na sigla em inglês). A presença desses dispositivos torna o raio de abrangência da proteção praticamente ilimitado. No ecossistema da cidade, além das tecnologias de IoT mais comuns, acabam coexistindo diversas tecnologias heterogêneas, protocolos de comunicação, mecanismos ciberfísicos (controlados por algoritmos e integrados à Internet), robôs, drones e veículos autônomos, tudo em linha com as tecnologias de nuvem correlatas, Big Data e inteligência artificial. Além disso, é essencial identificar e considerar as interdependências entre sistemas, já que um sistema de baixo risco pode estar interligado a outros ou ser de alto risco em determinados contextos. Da mesma forma, de acordo com a ENISA (2015), deve ser levado em consideração o problema dos ciclos de vida prolongados dos equipamentos utilizados ou dos sistemas legados, que raramente cumprem com a segurança projetada. Isto deve ser solucionado por meio de um plano de investimento (OSPI, 2017: 8).

É preciso mapear a grande variedade de atores públicos e privados que interagem e os que precisam ser coordenados e dotados de governança:

- Alta administração.
- Setores da cidade mais especializados em tecnologia, cibersegurança e proteção de dados.
- Áreas de competência em segurança (polícia, segurança do trabalho, etc.).
- Áreas setoriais mais envolvidas na digitalização (finanças, transporte, coleta e tratamento de resíduos, saúde, suprimentos, etc.).
- Superestruturas de cooperação ou coordenação criadas nos níveis local, regional ou nacional.
- Responsáveis pelos diversos níveis de serviços, infraestrutura, comunicações, etc., que muitas vezes são prestadores de serviços e de comunicações para terceiros e geralmente são do setor privado (água, eletricidade, mobilidade e transporte, segurança, etc.).
- Entidades do setor público que ocasionalmente também prestam serviços à cidade.
- Terceiro setor, organizações não governamentais (ONGs) ou instituições universitárias, que podem ser integradas a processos de análise ou participação (Muñoz et al., 2016: 26).
- Os cidadãos, que são os destinatários dos serviços e, ao mesmo tempo, constituem o grupo ao qual pertencem os dados que alimentam a cidade, são os que mais sofrem com os eventuais ataques ou falhas nos serviços.

Christina Wocin

2.2
Definir a governança da cibersegurança

Com base na identificação dos ativos, dados e processos a serem protegidos e dos atores a serem coordenados, é necessário estabelecer um esquema claro de governança da cibersegurança.


Mahdis Mousavi

2.2.1
Estabelecer a governança da cibersegurança e integrá-la à governança da cidade

A governança da cibersegurança se integra à da cidade inteligente, o que envolve a criação de normas e políticas, bem como a montagem de uma estrutura organizacional (MIAC, 2020). De acordo com o Fórum Econômico Mundial (FEM) (FEM, 2021), a governança de uma *smart city* envolve a integração de cinco políticas:

1. **Acessibilidade**, inclusão e impacto social.
2. **Segurança** e resiliência.
3. **Privacidade** e transparência.
4. **Abertura** e interoperabilidade.
5. **Política** de dados abertos e de *Dig Once* para garantir que a infraestrutura digital seja instalada com sustentabilidade operacional e financeira.

A governança e gestão da cidade e a cidade inteligente podem ser encaradas como o processamento e aproveitamento em massa de enormes quantidades de dados. Além disso, a **governança da cidade – e sua cibersegurança – deve ser integrada à governança mais ampla dos dados.** Isso implica, entre outras medidas, **a determinação das fontes de dados e de seu ordenamento e tráfico, das instituições e órgãos, das competências e responsabilidades e das diretrizes de gestão.** É necessário identificar os dados necessários e suas respectivas fontes, bem como determinar onde integrar, coletar, depurar e classificar, analisar e interpretar tais dados.

A governança da cibersegurança deve incluir a governança dos dados, o que pressupõe atribuir responsabilidades para a tomada de decisões sobre sua atualização, acesso, disponibilidade, propriedade, segurança e privacidade. Ela envolve também a determinação de diretrizes e padrões para sua gestão, qualidade e usos. A governança requer a gestão da arquitetura e infraestrutura dos dados, bem como a interoperabilidade e os protocolos para facilitar seu intercâmbio, interna e externamente, com outras administrações ou entidades privadas. A governança de dados também permite redefinir as competências profissionais e a gestão de recursos humanos, bem como atrair ou incorporar os perfis certos, além de permitir a transformação do modelo de gestão e de promover uma mudança cultural em todo o ecossistema.

Para a inovação e a *smart city*, o BID destacou **a importância de designar líderes** que gerem uma cultura de governança de dados, bem como de determinar poderes democráticos para a inovação (Townsend e Zambrano-Barragán, 2019: 41). **A criação de órgãos de governança ou sua regulamentação envia uma mensagem clara sobre a importância desse ponto.** Isso também pode gerar uma dinâmica de centralização de critérios e metodologias de coleta, processamento e aproveitamento de dados e de promoção de repositórios de dados compartilhados, ao mesmo tempo em que permite descentralizar ações específicas em relação a diferentes setores, o que facilita a coordenação e a interoperabilidade e permite dinâmicas transversais (Salvador, 2021).

Exemplos a serem seguidos sobre governança de dados:

- **Criação de órgãos: a Data Analytics (MODA) do gabinete do prefeito de Nova York, a Citywide Analytics Team de Boston, criadas em 2015, e o London Office of Data Analytics (LODA), de 2017. Na Espanha, a Oficina Municipal de Datos (OMD) da Prefeitura de Barcelona, instituída em 2018, e (no nível estadual) a División Oficina del Dato, que entrou em funcionamento em julho de 2020.**
- **Como exemplo de regulamentação, o Decreto 76/2020 da Catalunha, de 4 de agosto de 2020, regulamenta a governança da administração digital (arts. 5 a 9), bem como a governança de dados (Título II, arts. 10 a 26: modelo, protocolo, intercâmbio, interoperabilidade e acesso a dados, processos e serviços digitais, gestão de arquivos de dados e ativos digitais).**

As normas e esquemas de padronização e certificação a serem seguidos para alcançar uma cidade segura precisam ser integrados e alinhados com as políticas regionais e nacionais. **É necessário saber se o país conta com uma estratégia nacional de cibersegurança.**

Em 2004, a Assembleia Geral da OEA adotou a Estratégia Interamericana Integral de Combate às Ameaças à Cibersegurança (Barrero et al., 2018: 116). Muitos países da região adotaram estratégias nacionais de cibersegurança (Argentina, Brasil, Chile, Colômbia, Costa Rica, Guatemala, Jamaica, México, Panamá, Paraguai, República Dominicana e Trinidad e Tobago) (BID e OEA, 2020: 180).


Eddie Kopp

Infelizmente, essas estratégias em geral não levam em conta as cidades e não se aplicam diretamente a elas. Não obstante, **a cibersegurança urbana também faz parte da cibersegurança nacional.** A Aliança Global de Cidades Inteligentes do G20 (2021) destaca sua preocupação com a "má conexão com as políticas nacionais" da cibersegurança local. Soare e Burton (2020) falam sobre o "elo perdido" entre a cidade inteligente e a segurança nacional. ENISA (2015) recomenda que a "Comissão Europeia e os Estados-Membros esclareçam as responsabilidades de cada ator no caso de um incidente cibernético", e a Diretiva NIS da UE (Diretiva 2016/1148) segue essa mesma linha. A conexão entre a preparação para a segurança subnacional e a responsabilidade nacional ou federal foi objeto de análise no relatório de 2017 da Associação Nacional de Governadores dos EUA (Garcia, Forscey e Blute, 2017). Por sua vez, New America, Cohen e Nussbaum (2018) recomendam financiamento federal para simplificar os programas regionais ou locais e conectá-los às prioridades nacionais. Também é lembrado que as relações entre as autoridades regionais e as cidades são às vezes tão ou mais fragmentadas do que as nacionais ou federais.

Essa situação precisa ser corrigida nos níveis regional e nacional; entretanto ela representa também uma oportunidade para a cidade. **A cidade pode ser proativa e tentar conectar a cibersegurança urbana com a nacional.** Para tanto, devem ser identificados canais ou redes nacionais ou internacionais de cibersegurança. O leitor que tenha alguma responsabilidade nessa área deve considerar que sua cidade pode se tornar uma pioneira. É possível participar ou promover redes de boas práticas de cibersegurança entre as cidades. Pode ser possível, inclusive, descobrir a existência de programas de financiamento para a cibersegurança.

A cidade deve conhecer a legislação de cibersegurança que deve seguir. As regulamentações de cibersegurança podem ser diferentes em cada país. A regulamentação porventura existente deve ser seguida pelas cidades e por aqueles que fornecem bens ou serviços (tecnológicos e de telecomunicações) a ela. A União Europeia buscou homogeneidade e um padrão comum de cibersegurança. Assim, a Diretiva NIS obriga os Estados-Membros a adotar uma estratégia nacional e impõe obrigações aos fornecedores essenciais e aos operadores fundamentais, ou seja, aqueles cujas violações de segurança podem vir a gerar perdas financeiras significativas, abalar a confiança do público e até mesmo afetar a própria segurança nacional. Essas partes frequentemente operam e prestam serviços às cidades. São obrigadas a adotar medidas segundo os níveis de risco, com base em sua avaliação prévia. Por exemplo, esses provedores e operadores são obrigados a relatar incidentes de cibersegurança, mesmo os que não tenham tido qualquer efeito real, inclusive com o objetivo de fomentar uma cultura de gestão de riscos. Há uma plataforma comum de notificação que também pode ser usada para reportar violações de segurança de dados pessoais. O sistema é confidencial e protege a entidade notificadora e as pessoas que reportem incidentes, o que também pode envolver a cidade. As autoridades competentes exercerão funções de supervisão e fomentarão o desenvolvimento das obrigações.

Na Espanha, o setor público e as cidades devem seguir o Esquema Nacional de Segurança (Decreto Real 3/2010, de 8 de janeiro de 2010) e as Diretrizes de Segurança. Se a cidade não tiver uma legislação específica, esse esquema e essas diretrizes podem ser uma referência útil. Da mesma forma, a Diretiva NIS foi implementada principalmente por meio do Decreto-Lei Real 12/2018, de 7 de setembro de 2018, sobre segurança de redes e sistemas de informação, e do Decreto Real 43/2021, de 26 de janeiro de 2021, que especificou obrigações, indicadores e requisitos de segurança.

Em 2013, Singapura lançou seu plano diretor nacional de cibersegurança; em 2016 ele foi seguido por um projeto de lei de cibersegurança, aprovado e promulgado em 2018. Ambas as iniciativas faziam parte da Estratégia da Nação Inteligente de Singapura, que tem entre seus pilares exatamente a cibersegurança.[11]


George Kedenburg

Além da legislação obrigatória aplicável, a equipe de tecnologia deve estar ciente dos diversos padrões de cibersegurança e privacidade, bem como de suas adaptações para a IoT, as telecomunicações e as smart cities, e optar por seguir um deles naquilo que for possível. Nos últimos anos, foram desenvolvidas melhores práticas, bem como padrões e normas comumente aceitos. Para orientar as políticas de cibersegurança e de gestão de risco podem ser seguidas as estruturas padrão do setor, como as de organizações como a ENISA ou a NIST, bem como a ISO 2700, a AICPA, a CIS e a COBIT. Também deve ser dada atenção especial às normas de cibersegurança para a IoT e às telecomunicações provenientes dessas organizações, da União Europeia e da OTAN. Mais concretamente, com relação à *smart city*, a Organização Internacional de Normalização (ISO) já contava com a ISO 37120, referente a indicadores de serviços urbanos e qualidade de vida. Em 2017, a ISO 37120 e a ISO 37121, referentes a desenvolvimento sustentável e resiliência nas cidades, foram adotadas como modelo para o desenvolvimento das *smart cities*. Em 2019, foi lançada a ISO 37122, com indicadores do progresso de cidades inteligentes em economia, educação, energia, sustentabilidade, finanças, governança, saúde, habitação, população e condições sociais, recreação, segurança, resíduos, esporte e cultura, telecomunicações, transporte, agricultura urbana e segurança alimentar e gastos com água. Também podem ser adotados padrões de segurança específicos para o setor público e para a cidade. O quadro técnico do Capítulo 4 apresenta as diretrizes básicas que uma cidade pode seguir a partir desses sistemas.

11. Ver https://www.smartnation.gov.sg/about-smart-nation/secure-smart-nation/cybersecurity-public-sector.

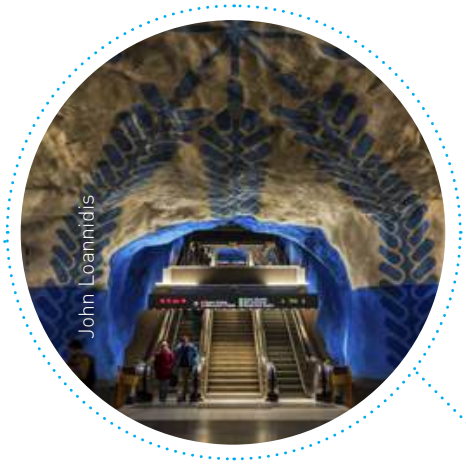
Na Estônia, foi criada em 2000 a ISKE, uma norma de segurança com a implementação de padrões organizacionais, de infraestrutura e medidas técnicas de segurança (Information System Authority, 2021), voltada para o setor público nacional e local.

Na Espanha, desde 2012 o Comitê Técnico de Normalização 178 da AENOR, sobre Cidades Inteligentes, e seus seis subcomitês (infraestrutura, indicadores e semântica, mobilidade e plataformas de transporte, energia e meio ambiente, destinos turísticos, governo e serviços públicos 4.0), já publicaram 31 normas de cidade inteligente (UNE, 2021). Essas normas facilitam a gestão e as estratégias da cidade inteligente e fornecem uma visão do estado de conservação durante todo o ciclo de vida dos diversos ativos e da infraestrutura tecnológica da cidade, inclusive riscos e respostas.

Por sua vez, Estocolmo, na Suécia, vem implementando desde 2010 diretrizes internas obrigatórias de segurança da informação, que seguem a ISO/IEC 27002. Além disso, são realizadas inúmeras atividades de conscientização sobre cibersegurança e desenvolvidos programas educacionais, além da oferta de apoio a laboratórios de pesquisa e inovação para start-ups.

Em 2014, a região de Rennes St Malo, na França, foi certificada com o selo French Tech, "Capital Tecnológica Francesa" (La French Tech, 2019), por ocupar o primeiro lugar em telecomunicações, agronegócio e cibersegurança, além de ter lançado o programa internacional de inovação Rennes Metropole, com sólidas parcerias comerciais e de pesquisa (Eurocities, 2016).

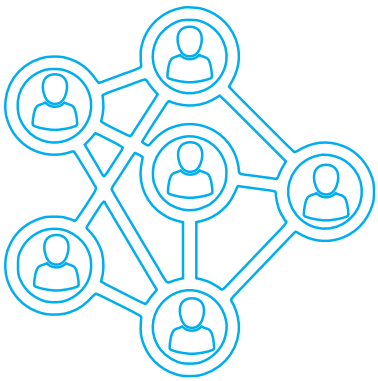

Dimitrina Kolarova


John Loannidis

2.2.2

Desenvolver políticas e padrões comuns de segurança com atribuições claras e comprometimento das partes

Com base na legislação pertinente e nas normas e modelos existentes, a cidade deve ser dotada de uma governança que integre dados, *smart city* e cibersegurança.



Em sua Recomendação 5, a ENISA (2015) sugere que os operadores, as cidades e as pessoas em busca de segurança para seus processos e serviços devem definir as responsabilidades da alta administração em matéria de cibersegurança; essa definição de responsabilidades pode ser um incentivo para aprimorar a cibersegurança. Da mesma forma, New America, Cohen e Nussbaum (2018) insistem na necessidade de identificação das funções, responsabilidades e poderes. Essa regulamentação deve ser uma indicação clara de apoio da liderança às iniciativas de cibersegurança e deve reduzir possíveis mal-entendidos e conflitos. É necessário um programa abrangente e centralizado das diversas partes envolvidas, não apenas as da área de tecnologia. É comum que ocorram conflitos entre os diversos órgãos para integrar a cibersegurança aos seus processos; entretanto, a solução pode vir de superestruturas de cibersegurança ou de um coordenador ou assessor dessa área.

Nessa linha, o Japão (MIAC, 2020) recomenda o seguinte:

I. Que suas cidades desenvolvam previamente padrões comuns de gestão de segurança, políticas de tratamento de dados e critérios de risco comuns para o conjunto.

II. Que suas cidades definam as atribuições de todas as partes; deve haver um acordo prévio sobre que organização registrará os incidentes e qual responderá a eles; se isso não for feito, poderá ocorrer a interrupção da prestação de serviços. Recomenda-se que sejam estabelecidos diagramas de configuração e de sistema e que se confirme que não há lacunas na administração.

III. Que todas as partes interessadas tenham sido conscientizadas e deliberado sobre os itens I e II, ou seja, políticas, normas e competências. Deve existir um fórum liderado pelo principal mantenedor, na medida do possível com a

participação de todos. Também em NIST (2019), observa-se a conveniência de obter consenso entre os líderes da organização, principalmente em relação às prioridades de proteção, privacidade e tolerância ao risco, bem como de alocar recursos para a implementação e monitoramento de controles.

Após o FEM, em junho de 2019, foi criada a Aliança Global de Cidades Inteligentes do G-20 sobre Governança Tecnológica, que reúne governos municipais, regionais e nacionais, parceiros do setor privado e da sociedade civil para compilar e analisar políticas para cidades inteligentes e éticas bem sucedidas. Já estão em vigor um roteiro e uma política de governança (FEM, 2020; 2021). Da ALC, estão participando as cidades de Bogotá, Brasília, Buenos Aires, Cidade do México, Córdoba (Argentina), Medellín, e San José.

A maioria (28 de 37) das smart cities pioneiras da Aliança Global de Cidades Inteligentes do G-20 adota políticas de responsabilidade cibernética. Um terço delas (13 das 28 cidades) designou um alto servidor para tratar dessa questão, e seus planos de governança são revistos anualmente. Além disso, metade delas (18 de 28) mantém um catálogo atualizado. A função de TI nem sempre é informada sobre a implantação de novas tecnologias (11 de 28) (FEM, 2021).


Mario Gogh

2.3
Institucionalizar a cibersegurança

A institucionalização da cibersegurança refere-se à forma de integrar e organizar entidades, recursos e o fluxo de informações com atribuições claras e participação das partes.

Para o BID (Bouskela et al., 2016), um dos quatro elementos da infraestrutura da *smart city* é o Centro Integrado de Operação e Controle (CIOC), comum em cidades com mais de 200.000 habitantes. Os CIOCs integram a estrutura tecnológica (computadores, sistemas de aplicativos e monitores de sistemas digitais), a infraestrutura física (salas de operação, gerenciamento de crises, etc.) e a infraestrutura de processos, bem como o pessoal e os representantes de diversos órgãos públicos e prestadores de serviços, utilizando uma abordagem colaborativa e abrangente das questões a serem tratadas no que deveria ser o cérebro da cidade inteligente. Esses centros são responsáveis pelo processamento e análise dos dados da cidade para a tomada de decisões inteligentes. Em algumas cidades, são o prolongamento de uma área setorial que impulsionou inicialmente a *smart city* – por exemplo, mobilidade, segurança e resposta a emergências – assumindo mais adiante outros objetivos e funções, como o gerenciamento de dados e de inteligência.

Toda cidade deve contar com um Centro de Operações de Segurança (SOC, na sigla em inglês), seja ele ou não um CIOC. Esse é um órgão primário de supervisão, que monitora a segurança das informações em tempo real, analisando quaisquer incidentes na atividade das redes, servidores, aplicativos, bases de dados, sites e outros sistemas. O SOC é também um sistema cooperativo sem descontinuidades, onde as informações são compartilhadas com diversos interessados, inclusive provedores e operadores comerciais dos diversos serviços prestados. Quando existente, o SOC integra e participa dos CSIRTs ou CERTs, que são as equipes que preparam, coordenam e dão resposta a incidentes de segurança e emergências de TI. **Dependendo das possibilidades da cidade, deve existir o objetivo de integrar a tecnologia, processos, pessoal e representantes de prestadores de serviços em um único centro. Essa integração deve também permitir o monitoramento em tempo real dos incidentes de segurança e o compartilhamento de informações entre as partes.**

Um exemplo em nível mundial, sobretudo no período que antecedeu a Expo 2020, desde 2013 Dubai tornou-se uma referência não apenas em inovação tecnológica, mas também em infraestrutura projetada e segurança estratégica. Em 2014, foi criado o Centro de Segurança Eletrônica de Dubai,[12] que conta com um departamento de cibersegurança em cada uma das 133 entidades governamentais e semigovernamentais. Além disso, anualmente, sua estrutura de governança de cibersegurança é revista pelo gabinete do diretor geral e avaliada pelo Centro de Segurança (Efthymiopoulos, 2016). Embora seja uma estrutura nacional, esse modelo pode inspirar projetos regionais e de grandes cidades.

12. Ver https://www.desc.gov.ae/about-us/#statement.

Yiran Ding

2.3.1

Nomear um gestor da cibersegurança

O Diretor de Segurança da Informação (CISO, na sigla em inglês) exerce uma função executiva com a atribuição de alinhar a segurança da informação com os objetivos institucionais e assegurar que a organização esteja protegida. Por sua vez, o Diretor de Informática (CIO, na sigla em inglês) é o diretor das TICs e responsável pelo seu alinhamento com as estratégias da organização (INCIBE, 2016).

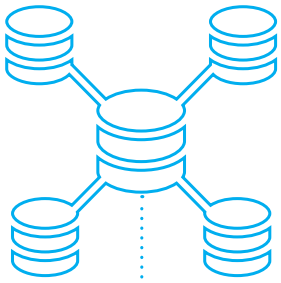
Há um consenso internacional no sentido de, tanto quanto possível, concentrar as responsabilidades de cibersegurança da cidade em um "servidor de alto nível", que pode ser considerado o CISO (FEM, 2020; G20 Aliança Global de Cidades Inteligentes, 2021). Entretanto, foram relatados casos em que os CISOs não tinham controle efetivo e direto. Se não for possível um modelo concentrado, é proposto um modelo de responsabilidade compartilhada entre uma equipe central de tecnologia da informação (TI), neste caso o CIO, os departamentos de operações da *smart city* e o gabinete do CISO. No Japão, observa-se que a responsabilidade pode ser compartilhada entre vários servidores de alto nível, desde que não surjam lacunas sem um responsável claro (MIAC, 2020). Nesses cenários, deve haver uma forte cooperação e coordenação entre o CISO e o CIO. New America, Cohen e Nussbaum (2018) advertem sobre os obstáculos para concentrar a cibersegurança em um indivíduo ou instituição, sobretudo em função dos sistemas e organizações legados e das dificuldades inerentes à integração de departamentos e serviços. De qualquer forma, eles enfatizam a conveniência de uma estrutura de cibersegurança ou de um coordenador ou assessor capacitado que se situe acima dos órgãos existentes para definir prioridades e coordenar ou direcionar esforços.

Dependendo das atividades identificadas para as capacidades de cibersegurança, deve ser considerada a formação de uma equipe mínima de cibersegurança, liderada pelo CISO, um executivo de proteção de dados pessoais, um especialista em testes de penetração e a equipe de apoio. O CISO deve se articular com a CIO da organização. Isso pode ser feito por meio de um comitê de cibersegurança. Esse comitê pode ter uma versão local para a entidade e outra em nível setorial. Para cada função, devem ser definidos perfis e competências genéricas (soft) e de cibersegurança (hard).

Em algumas cidades não há um CISO ou CIO; no máximo, pode haver um gestor de tecnologia. Assim, na medida do possível, suas responsabilidades devem ser concentradas e esclarecidas. Embora seja desejável contar com pessoal interno da própria cidade, algumas vezes os serviços especializados de um CISO podem ser terceirizados, como é o caso, em muitas cidades, dos representantes ou agentes de proteção de dados (AEPD, 2018).

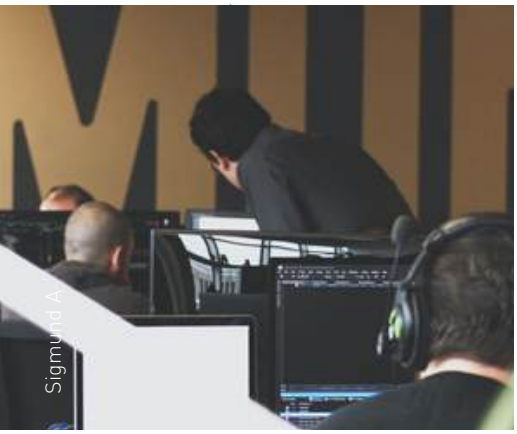
2.3.2

Determinar o papel do gestor de cibersegurança



Este alto servidor, ou CISO, **é responsável pelo cumprimento de todas as medidas de cibersegurança, especificamente aquelas dirigidas ao pessoal técnico,** bem como pela observância das normas e regulamentos pertinentes. É ele quem coordena a prestação de contas, com poderes para executar a cibersegurança de toda a infraestrutura de TI e tecnologia operacional (usuários, dispositivos, redes, dados e aplicativos). Ele deve ter uma conexão direta com a mais alta autoridade da cidade e ser membro da equipe de altos dirigentes do governo municipal ou se reportar diretamente a tal equipe. As principais funções do CISO são as "responsabilidades críticas" (Aliança Global de Cidades Inteligentes do G-20, 2021: 7 e seguintes), que podem ser encontradas na seção 4.3 deste guia.

Além disso, mas também sob sua égide, haverá gestores específicos responsáveis pela segurança de redes e aplicativos, monitoramento de ativos, registro da capacitação em segurança da informação e gestão de riscos (o que deve ser feito pelo menos anualmente), realização de auditorias ou designação de terceiros, implementação de uma política de avaliação de riscos e investigação dos terceiros com quem as atividades sejam terceirizadas, bem como responsáveis pela disponibilização para os cidadãos de materiais informativos sobre questões básicas de cibersegurança (Aliança Global de Cidades Inteligentes do G-20, 2021: 10 e seguintes).



2.3.3

Implementar mecanismos de compartilhamento de informações sobre ameaças cibernéticas com os diversos atores

Os atores públicos e privados devem compartilhar informações sobre incidentes de cibersegurança com confiança e sigilo, e com base em estruturas e pontos de contato e cooperação previamente definidos.

ENISA (2015) sinaliza que a troca de informações transversal e proativa sobre ameaças e incidentes é essencial para receber e poder dar respostas harmonizadas. A confiança entre as partes também é


Bermix

essencial para evitar danos reputacionais. Modelos de anonimização e confidencialidade podem ser úteis para tal fim. Entretanto, nas cidades inteligentes, geralmente não existe uma arquitetura de referência para o intercâmbio de dados. Devido a isso, NIST (2019) indica que é necessário consenso e a modificação das estruturas e processos existentes, bem como dos serviços compartilhados. Todas as partes interessadas devem instituir um ponto de contato para situações de emergência. No caso de provedores e prestadores de serviços, os contratos devem esclarecer e detalhar as informações a serem tratadas e destacar a responsabilidade e a comunicação entre as partes.

A cidade deve instaurar ou ter previsão de canais de comunicação de incidentes de cibersegurança entre as diferentes áreas ou serviços da própria cidade, bem como com todos os provedores e prestadores externos de serviços.

Como parte de suas responsabilidades, os líderes e gestores da cidade devem:

- **Definir** um ponto de contato para incidentes.
- **Divulgar** a existência de sigilo para os níveis técnicos e tecnológicos e para os prestadores de serviços que apresentarem informações.
- **Impor** obrigações de comunicação de incidentes nos contratos com os provedores.
- **Conduzir** exercícios com equipes pequenas que integrem diferentes áreas ou serviços urbanos, assim como com prestadores de serviços ou operadores, o que gera a dinâmica ou a confiança para o compartilhamento de informações.
- **Prever** também a comunicação com gestores em níveis regionais superiores ou nacionais.

Não há um modelo único a ser seguido. Os setores público e privado criaram sistemas de compartilhamento de informações de cibersegurança. New America, Cohen e Nussbaum (2018) apresentam as melhores práticas de governança de cibersegurança das *smart cities* e destacam os casos do Arizona (interface ACTRA), Nova Jersey (superestrutura burocrática NJCCIC, lugar comum que é um ponto de contato e coordenação), bem como o modelo do Escritório de Cibersegurança integrado à Washington Technology Solutions Agency (WaTech), que abrange capacidades de gestão militar e de emergências.


Jason Goodman

2.4
Integrar a segurança dos dados confidenciais da cidade à dos dados pessoais

2.4.1
Gestão dos dados

Cada vez mais, a cidade se beneficia das grandes quantidades de dados por meio de sua captura, coleta, armazenamento, análise e extração de valor para a tomada de decisões e prestação de serviços. Todos os dados e informações da cidade devem ser protegidos, mas isso deve ser feito de acordo com sua criticalidade e nível de risco. Para tanto, devem ser identificados e avaliados os dados essenciais, bem como aqueles particularmente confidenciais para a cidade. Para isso, **os regulamentos aplicáveis devem ser conhecidos e os dados devem ser avaliados na medida em que se relacionem com os bens, estratégias, interesses, funções e operações da cidade**. Também deve ser considerado se uma quebra na segurança desses dados poderia levar a danos diretos aos cidadãos, perdas econômicas, danos reputacionais ou protestos. Para essa identificação e avaliação, os níveis técnico e administrativo **contam com vários recursos** do NIST (2008), CCN (2020) ou OAS (2019). A partir daí, deve ser aplicado aos dados o nível de cibersegurança correspondente a seu valor e grau de risco.

Agora, cabe dar atenção especial aos dados pessoais e àqueles que merecem proteção especial. Em princípio, a maior parte dos dados tratados pela cidade não são de natureza pessoal, pois não podem ser vinculados a pessoas específicas. Entretanto, **são gerados cada vez mais dados pessoais**. Isso acontece devido à tendência à personalização de serviços e de visões em 360º, ou ainda em função da sensorização das pessoas e o uso crescente de apps da cidade em dispositivos celulares. Os dados de geolocalização, tão comuns na cidade inteligente, são particularmente sensíveis. Eles devem receber uma proteção ainda maior se estiverem ligados a reuniões ou manifestações políticas ou sindicais, centros médicos ou religiosos, padrões de comportamento relativos à vida sexual, etc. (AEPD, 2020b; ACS, 2011).

Os dados manejados pela cidade que puderem ser vinculados a cidadãos específicos são dados pessoais, de forma que se aplica a eles a ampla e rigorosa norma de proteção de dados. As garantias e exigências de segurança serão ainda maiores se, além disso, os dados receberem proteção especial (dados raciais, ideológicos, sindicais,

de saúde, genéticos, sexuais ou de identificação biométrica) ou se se referirem a crimes e sanções.

No caso dos dados pessoais, deve ser seguido o princípio de responsabilidade proativa: a cidade que maneje dados pessoais deve cumprir uma série de obrigações e ser capaz de comprovar que os cumpriu. Além disso, os processos e procedimentos da cidade que manipulem dados devem seguir os padrões de privacidade por projeto e por padrão. Sob o princípio da minimização, a cidade deve utilizar, desde o primeiro minuto, o mínimo de dados possível e pelo menor tempo possível. Isso contrasta com a mineração e aproveitamento de grandes volumes de dados, que é a própria essência da cidade inteligente. Minimização significa limitar a georreferenciação dos *smartphones*, sensores da cidade ou de *apps* da cidade ou de seus fornecedores. Além disso, é essencial depurar periodicamente as informações para evitar o acúmulo de dados que não atendam a propósitos legítimos ou que sejam desproporcionais. É necessário determinar os períodos de retenção de dados de acordo com seus objetivos, sensibilidade e riscos (AEPD, 2017; 12, 17). Transcorrido esse prazo, os dados não devem mais ser utilizados pela cidade, na medida do possível devem ser criptografados, e o acesso a eles deve ser restringido. Sempre que a legislação pertinente (sobre arquivos, transparência, responsabilidades administrativas ou autorizativas, etc.) o permita, os dados devem ser destruídos. Se possível, as cópias dos dados devem ser automatizadas.

Santander é uma das cidades inteligentes de referência na Espanha (por exemplo, em gestão de iluminação pública e coleta de lixo). Ela também se destaca por aplicar os conceitos de privacidade e segurança desde a fase de concepção do projeto. As empresas e os gestores da cibersegurança participam da definição das ações da cidade inteligente antes de sua execução e determinam as medidas a serem aplicadas. Por exemplo, devido à COVID-19, foi criado um sistema completo de controle do fluxo de pessoas nos edifícios municipais.

De acordo com o princípio de justiça, a cidade só pode manusear os dados para fins legalmente admissíveis e legítimos. De forma geral, os dados podem ser manuseados para fins de administração, gerenciamento fiscal, prestação de serviços sociais, educacionais ou de saúde, etc. O que não está claro é se a cidade inteligente pode reaproveitar tais dados para prestar melhor esses ou outros serviços, ou para avaliar, monitorar, controlar ou decidir políticas públicas, etc. Muitas vezes, as leis não são claras o suficiente em relação ao uso de dados pessoais pelas cidades ou, em termos específicos, para projetos de cidades inteligentes (como uma exceção positiva, vale mencionar a Lei de Economia Digital do Reino Unido de 2017,

seg. 35).[13] **É preciso assegurar que o projeto ou o processamento de dados pessoais tenha cobertura legal suficiente.**

Em todo o processamento de dados em massa realizado pela cidade, e antes da implantação de um projeto de cidade inteligente, **é obrigatório conduzir uma análise de risco e, muito provavelmente, uma avaliação completa do impacto da proteção de dados** (Art. 35 do Regulamento Geral de Proteção de Dados [RGPD];[14] AEPD, 2018; AEPD, 2020a: 22). Dessa forma, devem ser avaliadas as informações e o volume de dados a serem tratados, as fontes e a retenção, e determinados os riscos e impactos e, de acordo com eles, as medidas organizacionais e de segurança a serem adotadas. Em seu Guia para Avaliações de Impacto a AEPD (2021) explica como isso deve ser feito. **Em virtude de sua relação estreita e das semelhanças existentes na matéria, o cumprimento da proteção de dados deve estar ligado a ações de cibersegurança.**

O aproveitamento de dados pelas cidades tem se tornado cada vez mais intensivo e tem incorporado grandes camadas de inteligência artificial. Por esse motivo, devem ser levadas em conta salvaguardas e auditorias obrigatórias. Basicamente, deve ser administrada a qualidade dos dados de entrada e dos dados utilizados para treinar o sistema, deve haver controle dos vieses e da robustez do sistema de inteligência artificial, é preciso assegurar que sejam gerados registros ou logs que permitam verificar o funcionamento e as ocorrências e que a rastreabilidade, a transparência, a razoabilidade e a recorrência sejam monitorados; além disso, devem ser realizadas auditorias e avaliações constantes. Para isso, podem ser seguidas as diretrizes de inteligência artificial da AEPD (2020a e 2021).

Cabe destacar a criação, em 2020, do Registro de Algoritmos[15] da Cidade de Amsterdã, que proporciona ao cidadão um elevado grau de transparência sobre o uso da inteligência artificial na cidade inteligente e fornece descrições gerais e técnicas, além da possibilidade de participar de iniciativas.

Além disso, em 30 de junho de 2021, Barcelona, Londres e Amsterdam criaram o Observatório Global de Inteligência Artificial, destinado a monitorar a aplicação ética da inteligência artificial nas cidades. A ONU Habitat e o Centro para Assuntos Internacionais de Barcelona (CIDOB) colaboram com a iniciativa.

13. Ver https://www.legislation.gov.uk/ukpga/2017/30/section/35.
14. Ver https://www.boe.es/doue/2016/119/L00001-00088.pdf.
15. Ver https://algoritmeregister.amsterdam.nl/en/ai-register/?s=08.

Omar Prestwich

"Destaca-se a essência da cibersegurança: conhecimento e compreensão do ambiente, planejamento, proatividade na prevenção e vigilância constante, colaboração e cooperação, treinamento e capacitação permanentes."

2.4.2
Anonimização e pseudoanonimização, estratégias e medidas de segurança essenciais para que a cidade possa manejar os dados

Como salientado anteriormente, se faz mister identificar, avaliar e aplicar aos dados e informações as medidas de segurança correspondentes ao nível de risco. Contudo, cabe destacar que **muitas das dificuldades no cumprimento dos regulamentos de proteção de dados podem ser solucionadas se os dados puderem ser dissociados dos indivíduos específicos que os geram**. Esta é uma preocupação para os administradores das cidades, já identificada pelo BID (Cerdeira et al., 2020: 28). Para tanto, os dados devem ser anonimizados de acordo com as normas estabelecidas pelas autoridades de proteção de dados (AEPD, 2019a; ICO, n.d.). Se os dados forem anonimizados por completo, não há necessidade de aplicar regulamentos de dados e a cidade e seus provedores podem usá-los livremente e com menos medidas de segurança. Entretanto, a anonimização total é cada vez mais difícil, pois existem tecnologias cada vez melhores para reverter a anonimização e reidentificar as pessoas.

Uma estratégia fundamental é a pseudoanonimização. **A ideia é anonimizar os dados tanto quanto possível**, e que os diferentes serviços ou prestadores e empresas da cidade os manejem dessa forma para aproveitar e extrair seu valor sem o manuseio de dados pessoais. Ao mesmo tempo, os dados não pessoais permanecem isolados dos departamentos ou órgãos da cidade que tenham capacidade para reidentificá-los. Assim, em caso de violações ou vazamentos serão acessados somente os dados não pessoais. Além disso, **legalmente a pseudoanonimização torna muito mais fácil para a cidade aproveitar os dados de seus cidadãos para fins relacionados à cidade inteligente, estatísticas, pesquisas,** etc.

2.5
Integrar os provedores à cibersegurança

A cibersegurança deve ser incorporada à escolha, contratação e gestão de fornecedores e prestadores de serviços. Isso pode ser feito seguindo algumas diretrizes de compras, como as definidas recentemente para a área da saúde (ENISA, 2020).

Segundo o NIST (2019), **isso permite à cidade manter o controle e ditar os requisitos de gestão de riscos, e evita que sejam os fornecedores a impô-los a ela**. Entretanto, Ranchordás e Goanta (2020) advertem que as cidades acabam se curvando às condições estabelecidas pelas grandes plataformas, em detrimento dos valores e interesses comuns, da cibersegurança e dos direitos dos cidadãos. Nesse contexto, é aconselhável que as cidades compartilhem informações sobre fornecedores e prestadores de serviços e que definam cláusulas e contratos padrão. Soare e Burton (2020) consideram "paradoxal" que as compras públicas ainda não deem atenção suficiente à cibersegurança. As principais responsabilidades do CISO incluem a tomada de decisões de cibersegurança relativas a qualquer investimento significativo em produtos ou serviços de TI e tecnologia operacional adquiridos pela cidade. Shacklett (2019) ressalta que os regulamentos de segurança de TI devem ser aplicados de forma rigorosa. Fabricantes e fornecedores devem seguir abordagens de segurança desde o projeto das tecnologias e serviços adquiridos, como aquelas definidas de forma geral pela ENISA (2014): segurança prevista no projeto, menos privilégios (restrição de permissões), autenticação forte, proteção de ativos, segurança da cadeia de suprimentos, transparência da documentação, gestão da qualidade, continuidade do serviço e restrição do uso de dados.


Lagos Techie

Nas licitações e contratações, convém seguir as seguintes diretrizes:

- Incluir os requisitos de cibersegurança no Acordo de Nível de Serviço (SLA, na sigla em inglês) (FEM, 2021). Além disso, deve-se evitar o vazamento de informações no subempreiteiro (MIAC, 2020).
- Definir um plano específico de resposta a incidentes (Cerrudo, Asbini e Russell, 2015). Também deve ser incluído o suporte a incidentes 24 horas por dia, sete dias por semana.

- Determinar os testes aos quais o sistema será submetido e definir a exigência de certificações de terceiros. Também devem ser permitidos a auditoria e os registros, e os relatórios de auditoria de segurança devem ser apresentados anualmente.
- Definir como e por quem o cumprimento das obrigações de cibersegurança de terceiros e subcontratados será monitorado e controlado.
- Definir as informações que deverão ser compartilhadas, quais serão as funções e responsabilidades, etc. (MIAC, 2020). Deve ser detalhado um sistema eficiente de notificação e correção de vulnerabilidades que envolva os fornecedores (ENISA, 2015). Para isso, deve ser assegurada a interoperabilidade.
- Firmar acordos de confidencialidade que permitam o compartilhamento de informações sobre incidentes sem a necessidade de sua divulgação (NIST, 2019).

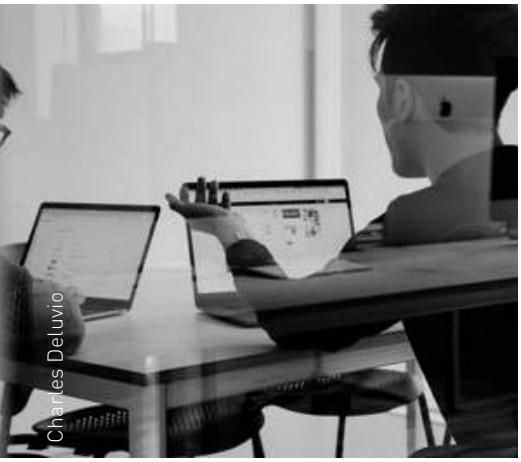
Forrest (2019) acrescenta **alguns elementos a serem considerados ao escolher um fornecedor**, como, por exemplo, se ele pode gerar publicidade negativa ou desconfiança entre os contratantes. Do ponto de vista financeiro, vale a pena considerar se ele é lucrativo, se tem outros clientes de grande porte e qual é sua estratégia de saída. Pode ser interessante chamar empresas especializadas em determinar o perfil dos fornecedores e seus riscos. Sem prejuízo de todas as precauções a serem tomadas, no caso de fornecedores emergentes em projetos piloto e de inovação, pode valer a pena flexibilizar as exigências.

Os regulamentos de proteção de dados muitas vezes exigem a inclusão de determinadas cláusulas nos contratos, vários aspectos das quais estão diretamente relacionados a medidas de segurança. Assim, os contratos da cidade com a empresa devem regular as relações entre o gestor (a cidade) e o processador (contratado) e detalhar as instruções, o dever de sigilo, as medidas de segurança aplicáveis, as possibilidades de subcontratação, os direitos dos sujeitos dos dados, as obrigações de colaboração, o destino ou eliminação dos dados após o uso, bem como os meios de que a cidade dispõe para controlar o cumprimento de tais condições. Isso pode ser feito com base no modelo e as Diretrizes de contratação da AEPD (2019). Deve ficar claro no contrato se as empresas utilizarão os dados para outros fins em interesse próprio, caso em que que elas se tornarão responsáveis ou corresponsáveis pela sua proteção.

2.6
Treinar, comunicar e conscientizar acerca da cibersegurança

A cibersegurança requer formação, comunicação e conscientização. Portanto, o alto gestor ou executivo municipal deve definir planos de treinamento, de conscientização e de comunicação.

2.6.1
Determinar os planos de treinamento


Charles Deluvio

De acordo com Stuart Chontos-Gilchrist, da E3 Technology, "as empresas estão reconhecendo que mais frequentemente são as pessoas, e não as máquinas, que criam violações na segurança".[16] Os *hackers* procuram sempre o elo mais fraco e os vetores de ataque geralmente incluem não apenas a tecnologia, mas também os servidores (ENISA, 2015, seção 5.1). O fator humano é determinante e as ameaças humanas são as mais relevantes (NCSC, 2021). Gestores e servidores precisam estar sensibilizados, treinados e atualizados para ter um bom desempenho (Bouskela et al., 2016: 45; Shacklett, 2019).

O executivo sênior responsável pela cibersegurança é também responsável pela **capacitação regular dos servidores, que deve ser bem planejado e dotado de recursos**. Como destaca Stilgherrian (2019), o treinamento em segurança é inútil se não houver comprometimento e mudança de comportamento. É preciso buscar o comprometimento e a mudança cultural. Para tanto, é essencial, em primeiro lugar, treinar as pessoas em segurança eletrônica pessoal (redes, família, casa, menores, assédio, etc.). Dessa forma, será muito mais fácil envolvê-las nas questões de cibersegurança e nas boas práticas da organização, como não repetir ou compartilhar senhas, atualizá-las frequentemente, não responder a mensagens suspeitas, não enviar informações por meio de canais não seguros, não utilizar equipamentos públicos para fins privados (e vice-versa), não instalar *software* não autorizado em seus dispositivos, etc. Deve-se levar em consideração a conveniência de estimular o compartilhamento de experiências e temores de segurança com os colegas (ver a experiência "*It's time to #askoutloud about cyber safety, Stay Smart Online*", do governo australiano).[17]

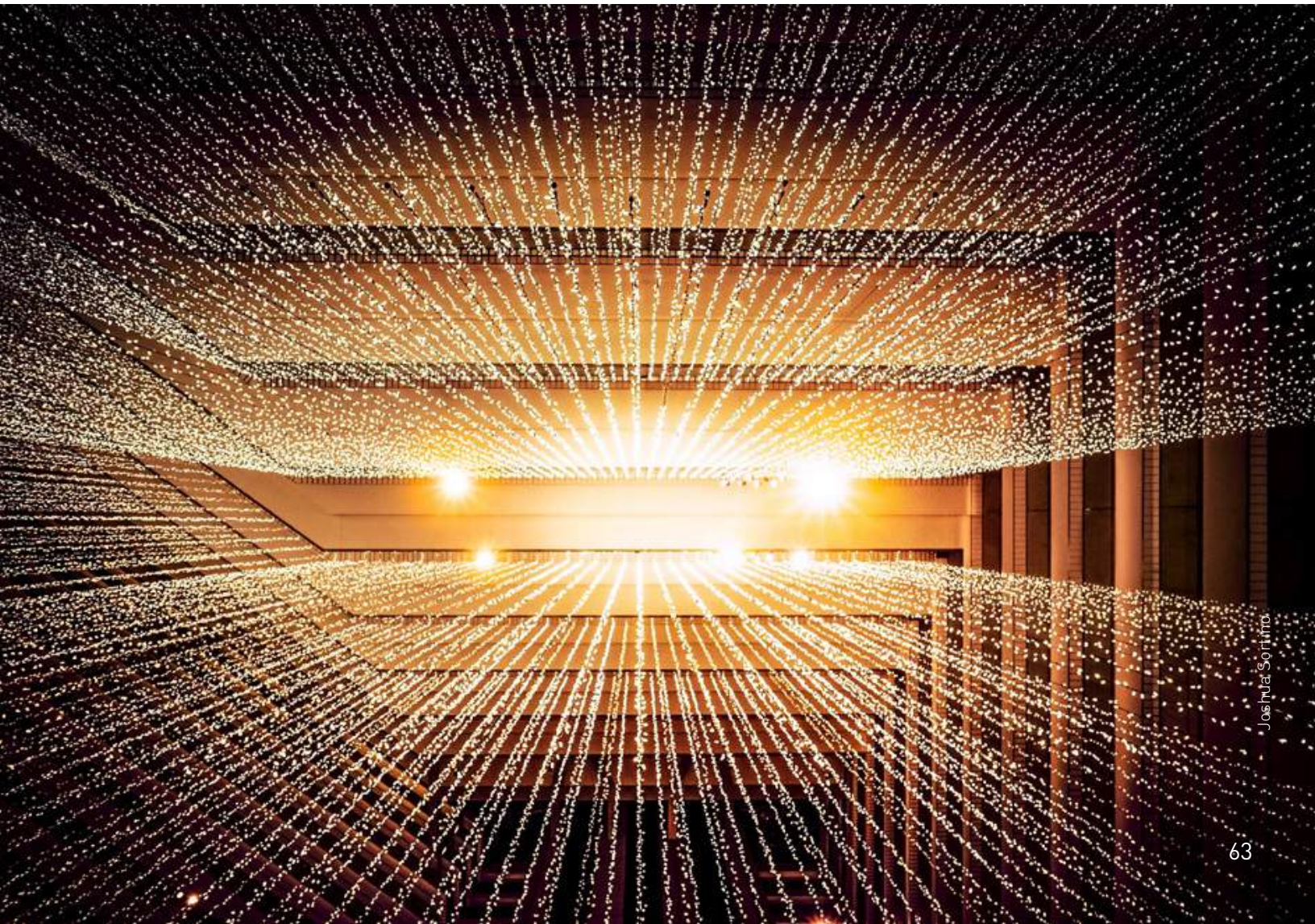
16. Ver https://www.e3security.com/about.

17. Ver https://www.acic.gov.au/media-centre/media-releases-and-statements/its-time-askoutloud-about-cyber-safety.

2.6.2
Determinar os planos de comunicação

Os gestores da segurança precisam explicar as tecnologias, políticas e práticas de cibersegurança em linguagem clara, que possa ser compreendida pelo prefeito, pelos gestores municipais e por executivos de fora da área tecnológica. A administração deve entender por que está promulgando regulamentos ou políticas, ou fazendo grandes investimentos. Se não os entenderem, não poderão explicá-los nem defendê-los. Obviamente, isso deve acontecer sem que haja a necessidade de que ocorra um problema de segurança para tornar tudo isso evidente.

A comunicação descendente é igualmente importante. **As políticas e regulamentos de cibersegurança são áridos, complexos e nem um pouco motivadores para os servidores.** É preciso investir na sua boa divulgação e, como mencionado acima, conseguir que o pessoal se responsabilize pelos focos de preocupação.



Joshua Sortino

2.7

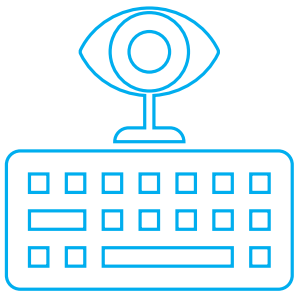
Dispor de financiamento e seguros para a cibersegurança

Uma cidade inteligente requer estabilidade financeira (Townsend e Zambrano-Barragán, 2019: 39) **e a cibersegurança necessita de verbas orçamentárias; se tais verbas não forem alocadas tempestivamente, essa necessidade aumenta cada vez mais. Os custos sociais, políticos, econômicos e de confiança de não investir em tempo hábil podem ser imensos.** ENISA (2015) observa que a conscientização e os gastos com cibersegurança são relativamente baixos em comparação com os impactos de eventuais ataques (como os descritos na seção 1.4.3); portanto, sua Recomendação nº 7 é que os operadores, provedores e municípios invistam mais em cibersegurança, sobretudo para aumentar a conscientização e oferecer treinamento para todo o pessoal e a alta administração, além de levá-los a desenvolver conhecimentos, etc., bem como para facilitar o recebimento de soluções de terceiros compatíveis com os requisitos de segurança.

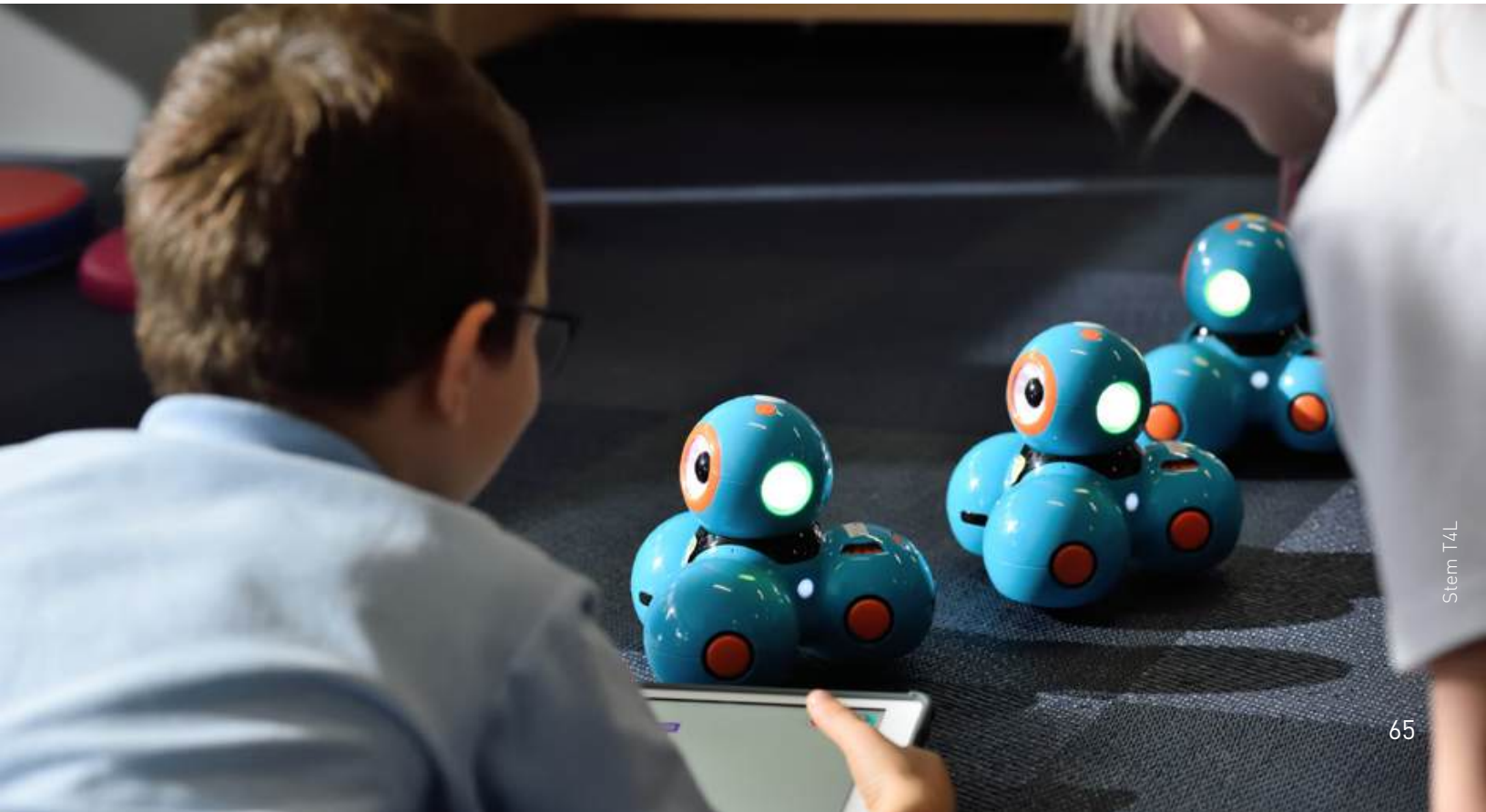
Os recursos precisam ser planejados e é preciso considerar também as revisões do projeto do sistema, testes, supervisão ativa do tráfego da rede, seguros e os custos técnicos, contratuais e jurídicos associados à correção e recuperação de uma violação. Sistemas obsoletos e desatualizados colocam em risco a cibersegurança. Soare e Burton (2020) apontam que os períodos prolongados de austeridade orçamentária implementados a partir de 2010 foram negativos, e a desaceleração econômica resultante da crise da COVID-19 pode agravar ainda mais a situação.

Na fase inicial, a cidade também deve considerar a possibilidade de **contratar um seguro de cibersegurança** e, é claro, integrá-lo a seus orçamentos. De acordo com uma pesquisa do *Wall Street Journal*, a maioria das 25 maiores cidades dos Estados Unidos contam com seguro cibernético ou estão considerando adquiri-lo (NIST, 2019). Os seguros podem cobrir os danos (inclusive reputacionais) causados por um ataque. Eles podem cobrir o custo dos serviços necessários para minimizar os danos, recuperar dados e equipamentos, proteger identidades e responder a reivindicações de terceiros. De forma similar, **quando uma cidade conta com seguro, também pode ser gerada uma dinâmica preventiva positiva**. Normalmente, os seguros incluem alguns serviços preventivos e de consultoria de conformidade. Além disso, eles impõem obrigações preventivas de cibersegurança. Consequentemente, além de minimizar os danos

em caso de ataque, a contratação de seguros estimula avaliações regulares, treinamentos, atualização de equipamentos, preparação de backups e outras medidas.



Até o momento, foram apresentados recursos, recomendações e melhores práticas para reagir às ameaças cibernéticas à cidade. O primeiro passo é levar em conta a complexidade do ecossistema e seus diversos atores. Foram descritas as principais diretrizes para políticas, normas, órgãos, responsabilidades e fórmulas de governança adequadas, com uma boa conexão com os níveis de cibersegurança regional e nacional. A cidade maneja muitos dados pessoais e confidenciais e precisa analisar os riscos e implementar medidas de segurança compatíveis com eles. A anonimização e a pseudoanonimização dos dados foram sugeridas enfaticamente como estratégia básica jurídica e de segurança. Foi enfatizada a importância do compartilhamento de informações entre as partes e destacadas as características necessárias para a seleção e contratação de provedores e fornecedores. Em qualquer caso, a conscientização e o treinamento dos servidores municipais continua sendo um dos maiores investimentos a serem feitos. Tudo isso exige recursos e orçamentos. O roteiro resumido mostrado na Figura 2.2 é adequado a todos os tipos de cidades: não há necessidade de esperar até amanhã para colocá-lo em prática.



Stem T4L

Figura 2.2.

Roteiro das responsabilidades de segurança cibernética urbana

Líderes do governo

1. Definir a visão e os objetivos de sua iniciativa de segurança cibernética; para tanto, definir o(s) setor(es) abrangido(s).
2. Estabelecer as normas e políticas necessárias: acordos, portarias, decretos, resoluções ou atos administrativos, alinhados com a estratégia regional e nacional de segurança cibernética; incorporar os padrões às normas.
3. Criar a estrutura institucional de aplicação da segurança cibernética, determinar os responsáveis e suas funções e definir um esquema de coordenação para lidar com incidentes.
4. Organizar as linhas de identificação e avaliação dos dados essenciais, bem como dos dados altamente confidenciais para a cidade.
5. Definir uma diretriz municipal para que a segurança cibernética seja integrada ao processo de seleção, gestão e contratação de prestadores de serviços.
6. Definir uma diretriz municipal para avançar nos processos de capacitação e comunicação.
7. Definir uma diretriz municipal para avançar nos processos de financiamento e aquisição de seguros.

Gestores municipais

1. Identificar os serviços a serem protegidos, definir os planos, programas e projetos alinhados às políticas do lado da equipe técnica e identificar os atores envolvidos.
2. Gerar os processos para o cumprimento e aplicação das normas e políticas.
3. Definir processos e procedimentos internos para a criação da estrutura institucional do setor.
4. Definir processos e procedimentos internos para a identificação e avaliação dos dados essenciais, bem como dados altamente confidenciais para a cidade.
5. Integrar a segurança cibernética ao processo de seleção, gestão e contratação de prestadores de serviços.
6. Instaurar um plano de capacitação e comunicação no setor.
7. Estabelecer um plano de financiamento no setor e a aquisição de seguros.

Pessoal de tecnologia da informação

1. Identificar informações associadas aos serviços e ativos de apoio a serem protegidos.
2. Cumprir e executar as normas e políticas estipuladas para a função de segurança cibernética; identificar o modelo dessa segurança a ser implantado.
3. No âmbito do modelo de segurança cibernética, definir as capacidades a serem implantadas; para tanto, os processos, tecnologia e informações deverão ser integrados à estrutura institucional.
4. Identificar e avaliar os dados essenciais, bem como os dados altamente confidenciais para a cidade.
5. Definir os requisitos básicos de segurança a serem incorporados ao processo de aquisição de produtos e serviços seguros de tecnologia.
6. Executar o plano de capacitação e comunicação da iniciativa.
7. Executar o plano de financiamento de acordo com o roteiro traçado e os recursos atribuídos.

Fonte: Elaboração própria (2021).
Observação: As responsabilidades apresentadas nesta figura devem ser articuladas com as responsabilidades a serem definidas para o pessoal de nível médio pelos líderes e gestores municipais e, por sua vez, entre eles e o pessoal de cibersegurança e TI.

3 Decálogos de cibersegurança para o pessoal de nível estratégico, tático e operacional ou técnico

Ruslan Bardash

"A cibersegurança está nas mãos de administradores, secretários e servidores que conduzem ações específicas para executar políticas, planos e programas e se aprofundam em cada área específica da cidade."

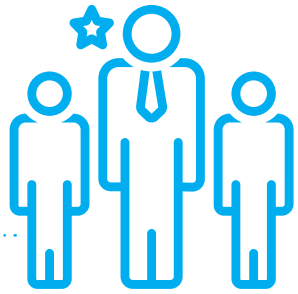
3.1
Decálogo para prefeitos e altos dirigentes

Líderes governamentais – Nível estratégico

A cibersegurança depende da direção executiva geral, bem como da visão, liderança, ação estratégica e definição de objetivos com determinação de políticas e gestão de recursos. Em função disso, cabe destacar as seguintes recomendações:

1. **Gerar acordos políticos** com diversos setores. A cibersegurança é uma política de toda a cidade que vai além de um simples mandato eleitoral; ela exige consenso, recursos e uma visão de médio e longo prazo, o que facilitará a priorização e a alocação dos recursos necessários a essa área.
2. **Enviar mensagens políticas destinadas a sensibilizar** servidores e cidadãos visando obter apoio político. Não é necessário esperar a ocorrência de um ataque cibernético para compreender seu impacto.
3. **Reunir toda a política de cibersegurança** em uma só voz. Fazer com que as partes envolvidas adotem estratégias, políticas, normas e competências claras em matéria de cibersegurança. Por meio de sua liderança, o prefeito ou a pessoa responsável outorgam legitimidade e reforçam as medidas destinadas a unir as diversas áreas dos setores público e privado.
4. **Estabelecer institucionalidade** e considerar a criação, no campo da cibersegurança, de uma área de coordenação e de centros de controle com responsabilidades bem definidas. Dotá-los de recursos e dar apoio especial à sua integração e cooperação.
5. **Estimular a conscientização**, capacitação e treinamento contínuos em cibersegurança para servidores e gestores, e assegurar que sejam conduzidas campanhas para os cidadãos. A cibersegurança depende de todos. Assegurar que as normas, políticas e planos não sejam engavetados, e estimular testes, simulações e avaliação contínua.
6. **Envolver as entidades do setor privado** que fornecem bens e serviços para a cidade. Manter esquemas de coordenação e confiança. Assegurar que o governo municipal determine os termos de contratação e que elas incorporem a cibersegurança, inclusive no caso de start-ups e pequenas e médias empresas (PMEs), por meio de políticas, planos e financiamentos.
7. **Estimular a atualização e renovação de ativos tecnológicos** obsoletos e a aquisição de bens e serviços que incorporem a segurança em seus projetos, automatizem a cibersegurança e empreguem tecnologias emergentes.
8. **Assegurar que a cibersegurança seja parte dos elementos a serem avaliados** nas políticas da cidade, sobretudo nas cidades inteligentes.
9. **Empregar mecanismos de planejamento financeiro** que permitam manter projetos de curto, médio e longo prazo. Ter sempre em mente que a cibersegurança necessita de recursos e de verbas.
10. **Fomentar a participação do município nas redes nacionais de cibersegurança** para cidades. Os programas locais de cibersegurança devem ser alinhados às estratégias metropolitanas e nacionais. Dedicar atenção especial aos recursos oferecidos nos níveis nacional, federal e até mesmo internacional.

3.2
Decálogo para secretários e servidores municipais



Gestores municipais – Nível tático

Sem prejuízo das decisões estratégicas, a cibersegurança está nas mãos de administradores, secretários e servidores que conduzem ações específicas para executar políticas, planos e programas e se aprofundam em cada área específica da cidade. As recomendações a seguir são aplicáveis a eles, segundo seu cargo e suas responsabilidades:

1. **A cibersegurança começa com cada um**, em seu computador e em seu dispositivo móvel. Identificar perfeitamente a tecnologia e a infraestrutura a serem protegidas das ameaças digitais, bem como os atores envolvidos.
2. **Conhecer e entender as ameaças** às quais se está exposto no espaço digital. Na medida do possível, realizar uma autoavaliação ou diagnóstico do nível de maturidade em cibersegurança.
3. **Conhecer as medidas concretas, estratégias**, padrões, políticas e procedimentos de cibersegurança que sua cidade adota e quais são suas responsabilidades. Assegurar que os subordinados estejam cientes das questões de cibersegurança sob a alçada de seu superior hierárquico.
4. **Não engavetar políticas e normas.** Testar suas próprias responsabilidades, participar de simulações e adotar processos e procedimentos. As eventuais falhas de segurança detectadas na prefeitura ou na empresa prestadora de serviços devem ser comunicadas ao órgão competente, inclusive de forma confidencial.
5. **Participar de programas de treinamento** e atualização para desempenhar as responsabilidades de cibersegurança.
6. **Comunicar bem as políticas e diretrizes** para que sejam de responsabilidade de todos. Compartilhar suas próprias experiências de cibersegurança com seus colegas, com outras áreas e com outros governos locais.
7. **Verificar a disponibilidade de recursos materiais**, humanos, financeiros e técnicos necessários para desempenhar as responsabilidades de cibersegurança. Se forem insuficientes, planejar e solicitar a dotação dos recursos necessários.
8. **Se apropriado, planejar e estruturar os recursos humanos**, recrutando pessoal adequado para as áreas de cibersegurança e novas tecnologias.
9. **Na medida do possível, buscar a cooperação com fornecedores** e prestadores de serviços privados, interagir com eles e criar um clima de confiança que permita o compartilhamento de informações críticas de cibersegurança.
10. **Assegurar que os contratos** com fornecedores incluam obrigações, documentação e serviços de resposta adequados, além de que sejam claros em relação aos requisitos de segurança e de verificar seu cumprimento.

3.3
Decálogo para pessoal técnico de cibersegurança e de TI

Nível operacional

As recomendações a seguir são direcionadas aos gestores que estejam familiarizados com as tecnologias e sistemas para proteção da cidade. Essas pessoas seguem as estratégias e táticas formuladas em outros níveis e propõem diretrizes técnicas e de capacitação e os procedimentos para gerenciamento, identificação, proteção, detecção, resposta e recuperação de incidentes. Geralmente, é o pessoal de TI que assume a liderança da cibersegurança, embora às vezes haja especialistas com responsabilidades específicas por essa segurança. As recomendações incluem:

1. **Determinar o escopo** e os serviços e sistemas a serem assegurados, sobretudo aqueles sob sua própria responsabilidade, e deixar claro quais são os órgãos e atores dos quais eles dependem.
2. **Estar ciente das diretrizes**, estratégias, políticas, normas e boas práticas definidas na cidade e operacionalizá-las nos sistemas sobre os quais tenha responsabilidade.
3. **Em um processo contínuo, participar e contribuir para a avaliação,** gestão e planejamento da cibersegurança.
4. **Identificar os órgãos e responsabilidades** específicos de cibersegurança da entidade onde trabalha e conhecer suas responsabilidades por incidentes e pela resposta a eles.
5. **Realizar uma autoavaliação** ou diagnóstico do nível de maturidade das capacidades da cidade de acordo com as ferramentas disponíveis e, a partir daí, dimensionar as capacidades e recursos necessários.
6. **Na medida das responsabilidades assumidas, planejar** e determinar medidas concretas para atingir os objetivos.
7. **Proteger e implementar sistemas de identificação**, autenticação e controle de acesso, bem como mecanismos de detecção de anomalias e monitoramento para a resposta a incidentes.
8. **Se fizer parte das funções atribuídas, assegurar** que, por padrão, a aquisição de bens e serviços de tecnologia pela cidade contemple a segurança e a privacidade. Manter-se a par dos novos métodos e ferramentas de ataque. Atualizar e aprimorar as ferramentas de *hardware* e *software*. Se possível, optar por sistemas automatizados de detecção e resposta a ameaças. Se fizer parte de suas responsabilidades, manter-se um passo à frente e criar equipes de segurança ofensiva ou ativa para antecipar-se aos ataques.
9. **Com base nas funções definidas nos processos e procedimentos, determinar os perfis da equipe** que será responsável pela função de cibersegurança.
10. **Integrar políticas de privacidade** e proteção de dados às políticas de cibersegurança.

4

Capacidades técnicas para proporcionar cibersegurança à cidade

Augusto Navarro

"Entre os compromissos a serem assumidos está a obediência às normas, políticas e diretrizes estabelecidas para a função de cibersegurança."

4 Capacidades técnicas para proporcionar cibersegurança à cidade

Os leitores deste guia já compreenderam os perigos, ameaças digitais, atores, motivações e o impacto dos ataques cibernéticos às cidades e, portanto, a necessidade de levar a sério a cibersegurança urbana. Para isso, eles já dispõem de recursos, melhores práticas e recomendações que lhes permitirão enfrentar essa missão. Entretanto, a cibersegurança tem um componente técnico inevitável, e esta seção é destinada especificamente aos decisores e ao pessoal de tecnologia encarregado da cibersegurança da cidade, a quem é fornecido um roteiro para a implementação de modelos de maturidade de capacidades. Entre os compromissos a serem assumidos está a obediência às normas, políticas e diretrizes estabelecidas para a função de cibersegurança (Figura 4.1).

Figura 4.1.

Diretrizes para o pessoal de cibersegurança e tecnologia da informação

1. **Identificar** informações associadas aos serviços e ativos de apoio a serem protegidos.
2. **Cumprir** e executar as normas e políticas estipuladas para a função de segurança cibernética; identificar o modelo dessa segurança a ser implantado.
3. **No âmbito do modelo de segurança cibernética, definir** as capacidades a serem implantadas; para tanto, os processos, tecnologia e informações deverão ser integrados à estrutura institucional.
4. **Identificar** e avaliar os dados essenciais, bem como os dados altamente confidenciais para a cidade.
5. **Definir** os requisitos básicos de segurança a serem incorporados ao processo de aquisição de produtos e serviços seguros de tecnologia.
6. **Executar** o plano de capacitação e comunicação da iniciativa.
7. **Executar** o plano de financiamento de acordo com o roteiro traçado e os recursos alocados.

Fonte: Elaboração própria (2021).

O objetivo primordial do roteiro é implantar e reforçar capacidades, o que permite o lançamento de iniciativas de médio e longo prazo. As capacidades são definidas com base no modelo de maturidade da capacidade de cibersegurança escolhido (Tabela 4.1). Dependendo de suas necessidades, o pessoal técnico pode optar por um dos diversos modelos de maturidade.

Tabela 4.1.

Modelos de maturidade de cibersegurança para organizações

Acrônimo	Nome	Proposto por	Níveis de maturidade
CCSMM	Modelo de maturidade da cibersegurança comunitária	White	5
COBIT	Objetivos de controle para a informação e tecnologia correlata	ISACA	5
CSF-NIST	Marco de cibersegurança	NIST	5
C2M2	Modelo de maturidade da capacidade de cibersegurança	Curtis	4
ISMS	Sistema de gestão da segurança da informação – ISO/IEC 27001	ISO/IEC	5
ISM3	Sistema de gestão da segurança da informação – Modelo de maturidade	ISM3	5
-	Modelo de maturidade da capacidade de cibersegurança da Iniciativa Nacional para Educação em Seguridade Cibernética (NICE)	US DHS	3
RMM	Modelo de gestão da resiliência	CERT	4
SSE-CMM	Modelo de capacidade de engenharia de segurança de sistemas	NSA	5

Fonte: Adaptado de Rea-Guaman et al. (2017).

O desenvolvimento e a implantação de capacidades técnicas podem ser agregados em uma "função de cibersegurança" que inclua **a gestão** (reengenharia de processos e definição das funções fundamentais); **formação do pessoal**, capacitação e gestão de mudanças; **atividades técnicas** (sistemas de informação, ou *software*, e a infraestrutura que lhes dá sustentação, ou *hardware*); e finalmente **a gestão de informações** (conectando processos com a TIC, as tecnologias digitais e as tecnologias emergentes). O pessoal de TI é responsável por essa função de cibersegurança e deve seguir estas três etapas: autoavaliação das capacidades, identificação das capacidades a serem desenvolvidas e operação da função de cibersegurança.

4.1
Etapas da função de cibersegurança

Como observado acima, a função de cibersegurança é desenvolvida em três etapas (ver Figura 4.2).

Figura 4.2.

Etapas a serem cumpridas para a implantação da função de cibersegurança

1. **Autoavaliação de capacidades**
2. **Identificação de capacidades a serem desenvolvidas**
3. **Funcionamento da função de segurança cibernética**

Fonte: Elaboração própria (2021).

A primeira etapa para **implantar a função de cibersegurança** implica um processo de **autoavaliação** e o diagnóstico do nível de maturidade das capacidades, de acordo com os instrumentos próprios do modelo escolhido e as informações associadas aos serviços e ativos de apoio que se pretende proteger. No caso deste guia, o autodiagnóstico está incluído no link **www.iadb.org/cibereval**, para o qual se usa como referência o modelo de cibersegurança da NIST, um dos mais utilizados. Não obstante, quaisquer dos modelos ou práticas adotadas poderia ser usado ou combinado em função dos serviços da cidade que se pretende proteger.

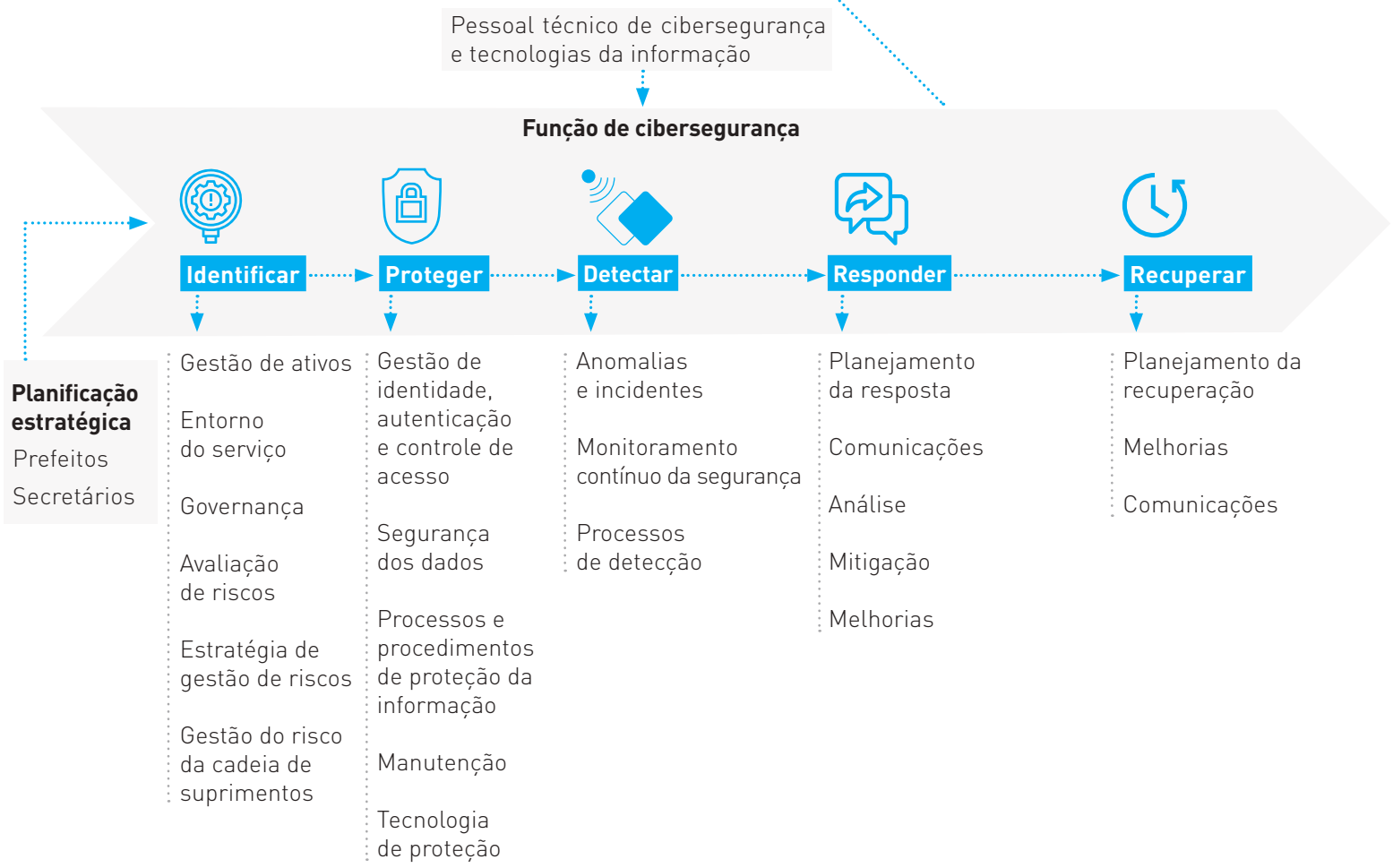
Entre outros objetivos, o processo de autoavaliação busca determinar o nível de maturidade a partir das seguintes perguntas:

1. **Que atividades devem ser realizadas?**
2. **Que informações são utilizadas ou produzidas nos processos?**
3. **Quem está envolvido nas capacidades?**
4. **Que tecnologia deve viabilizar essas capacidades?**

A segunda etapa é a **identificação** das capacidades que a função de cibersegurança **deve desenvolver** a partir dos resultados obtidos no autodiagnóstico. A determinação das capacidades estará vinculada à identificação, proteção, detecção, resposta e recuperação de incidentes que possam ocorrer nos serviços oferecidos.

Figura 4.3.

Identificação de capacidades em cibersegurança



Fonte: Elaboração própria; modelado a partir do marco de cibersegurança do NIST.

A terceira etapa é a entrada em **funcionamento** da função de cibersegurança. Como exemplo, pode ser mencionado o modelo Marco de Cibersegurança (Cybersecurity Framework) da NIST, que corresponde a ações específicas que miram **cinco capacidades**: identificar, proteger, detectar, responder e recuperar, cujos elementos são descritos a seguir de forma mais detalhada.

4.1.1
Identificar

Esta capacidade permite entender o contexto no qual se desenvolve o serviço da cidade, os recursos que respaldam as funções críticas e os riscos de cibersegurança relacionados à prestação de tal serviço. Ela possibilita a gestão dos riscos de cibersegurança em sistemas, pessoas, ativos, dados e capacidades. A seguir, são apresentadas as subcapacidades que compõem esta capacidade, de acordo com as categorias propostas pela NIST, para o quê se tomam como exemplo os serviços financeiros de uma municipalidade.

Identificar

- Gestão de ativos
- Entorno do serviço
- Governança
- Avaliação de riscos
- Estratégia de gestão de riscos
- Gestão do risco da cadeia de suprimentos

Identificar:

Os dispositivos e sistemas físicos, plataformas de *software* e aplicativos integrados à gestão financeira da cidade.

O *hardware*, dispositivos, dados, tempo, pessoal e o *software*, em função de sua classificação, criticidade e valor agregado aos serviços financeiros da cidade.

A cadeia de suprimentos integrada aos serviços financeiros.

Os requisitos legais e regulamentares relativos à proteção dos dados manuseados nas transações econômicas e financeiras da cidade.

Os impactos e a probabilidade de que os serviços financeiros sejam afetados por um ataque digital.

A estratégia de gestão de riscos para os serviços financeiros oferecidos.

Andy Holmes

4.1.2
Proteger

Abrange as subcapacidades que permitem desenvolver e implementar medidas de segurança adequadas para garantir a prestação dos serviços urbanos. Elas incluem a capacidade para limitar ou conter o impacto de um eventual evento de cibersegurança.

Proteger

- Gestão de identidade, autenticação e controle de acesso
- Segurança dos dados
- Processos e procedimentos de proteção da informação
- Manutenção
- Tecnologia de proteção

Implementar medidas de proteção como as seguintes:

Auditoria dos dispositivos utilizados.

Emissão de identidades, credenciais e autorizações para acessar os serviços financeiros da cidade.

Capacitação dos usuários vinculados ao serviços financeiros da cidade.

Mecanismo de comprovação de integridade para testar o *software*, o *firmware* e a integridade das informações.

Implementação de processos de controle de alterações da configuração dos sistemas que abrigam todas as informações financeiras da cidade.

Preparação e manutenção de *backups* das informações.

Implementação e gestão de planos de resposta a ataques digitais.

Proteção das redes de comunicações e controle.

Implementação de mecanismos (por exemplo, a prova de falhas, equilíbrio de carga, troca a quente [*hot swap*]) para cumprir os requisitos de resiliência em situações normais e adversas.

Christina Wocin

4.1.3
Detectar

Implica no desenvolvimento e implementação de medidas apropriadas para identificar a ocorrência de um evento de cibersegurança nos serviços da cidade.

Detectar

- Anomalias e incidentes
- Monitoramento contínuo da segurança
- Processos de detecção

Conduzir medidas de detecção como as seguintes:

Coletar informações e analisar os ataques detectados para entender os alvos e os métodos.

Determinar o impacto dos ataques.

Monitorar a atividade do pessoal, dos provedores e da rede para detectar possíveis eventos de cibersegurança.

Implementar mecanismos para identificar *software* não autorizado, códigos maliciosos, etc.

Aprovar os processos de detecção.

Vladimir Kudinov

4.1.4
Responder

Esta capacidade consiste no desenvolvimento e implantação de mecanismos apropriados para tomar providências relativas a incidentes de cibersegurança detectados.

Responder

- Planejamento da resposta
- Comunicações
- Análise
- Mitigação
- Melhorias

Colocar em funcionamento medidas de resposta como as seguintes:

Executar o plano de resposta durante e depois de um incidente.

Comunicar os incidentes às autoridades, de acordo com o esquema de coordenação definido pela instituição.

Investigar as notificações emitidas pelos sistemas de detecção.

Entender o impacto do incidente.

Efetuar perícias.

Incorporar as lições aprendidas aos planos de resposta.

Atualizar as estratégias de resposta em face do incidente.

Conter e mitigar os incidentes e vulnerabilidades identificados.

Documentar todo o processo, incorporar as lições aprendidas e atualizar o plano de resposta.

Álvaro Reyes

4.1.5
Recuperar

Esta capacidade abrange o desenvolvimento e implementação de medidas apropriadas para manter os planos de resiliência e restabelecer as capacidades ou serviços que tenham sido afetados por um incidente de cibersegurança.

Recuperar

- Planejamento da recuperação
- Melhorias
- Comunicações

As ações de recuperação devem incluir o seguinte:

Executar o plano de recuperação durante ou depois de um incidente de cibersegurança ter afetado os serviços financeiros da cidade.

Incorporar as lições aprendidas aos planos de recuperação.

Restaurar a reputação da entidade afetada após o incidente.

Comunicar as atividades de recuperação às partes interessadas internas e externas, bem como às equipes executivas e administrativas.

Sammy Ayot

4.2

Tecnologia da função de cibersegurança

A função de cibersegurança pode exigir diversos serviços de processamento de informação, inclusive serviços especializados de *hardware* e *software* para testes de penetração e serviços de monitoramento, auditoria e perícia de informática. É conveniente optar por sistemas automatizados.

IFLY:D

4.3

Funções do gestor máximo da cibersegurança

O gestor máximo desse campo deve desempenhar as seguintes funções:

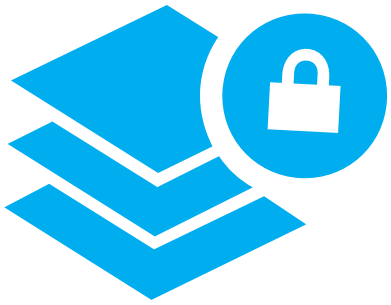
- Informar aos gestores municipais todos os assuntos relativos à cibersegurança e comunicar-se com as autoridades competentes.
- Definir o marco geral de governança e a política de cibersegurança, que será analisada e aprovada pelos altos dirigentes pelo menos uma vez por ano.
- Fazer cumprir a política de segurança de ativos e equipamentos, assegurar o cumprimento dos regulamentos pertinentes, supervisionar a revisão anual dos documentos de segurança da informação e os resultados das auditorias.
- Fazer um inventário e ter uma visão da infraestrutura tecnológica a ser protegida. Tomar decisões de cibersegurança relativas a todos os produtos, serviços, aquisições e desenvolvimento de aplicativos internos de TI e tecnologia operacional existentes.
- Conduzir avaliações de impacto de segurança e privacidade.
- Cooperar com os fornecedores do setor privado e zelar pela inclusão da cibersegurança nas contratações.
- Responsabilizar-se pela capacitação dos servidores e realizar avaliações anuais.
- Examinar e registrar todos os incidentes de segurança e adotar as medidas necessárias de acordo com um plano específico de resposta a incidentes e de recuperação de desastres. Em alguns sistemas, essa estratégia deve ser testada no mínimo uma vez por ano.

5 O BID e a cibersegurança nas cidades

Zhu Hongzhi

"O BID, na qualidade de parceiro estratégico, procura apoiar os países da região para enfrentar o novo desafio da cibersegurança urbana."

5 O BID e a cibersegurança nas cidades



O Grupo BID definiu a "Visão 2025, Reinvestir nas Américas" como o guia para auxiliar os países da ALC na recuperação dos efeitos da pandemia. Essa visão se baseia em cinco pilares de ação: 1) a transformação digital e a adoção mais rápida de tecnologia nos setores público e privado, 2) fortalecimento das cadeias de valor da região, 3) mudança do clima, 4) apoio às PMEs, 5) igualdade de gênero e inclusão. Com isso, busca-se impulsionar as oportunidades de crescimento sustentável, reativar a economia da região, fomentar o progresso social e reforçar a boa governança.

Há mais de uma década, o BID acompanha a região em sua transformação digital. Por meio do **Marco de Ação para a Transformação Digital**,[18] foi proposto o fortalecimento da gestão pública digital, a transformação digital dos serviços sociais e de infraestrutura, o desenvolvimento sustentável e a digitalização das cidades, bem como a transformação digital do setor privado.

A transformação digital e o uso de novas tecnologias e de grandes dados contribuem para a formulação de políticas públicas para responder aos principais desafios sociais e alcançar os Objetivos de Desenvolvimento Sustentável (ODS) das Nações Unidas.

A pandemia da COVID-19 acelerou a **transformação digital** dos países da região, mas são as **cidades** que enfrentam o maior desafio para assegurar a continuidade do fornecimento de bens e serviços aos cidadãos.

A transformação de uma cidade para a adoção de um modelo de gestão mais inteligente, com tecnologias digitais, aumenta a vulnerabilidade dos ativos no espaço digital.

A cibersegurança é, portanto, uma questão emergente e crucial no que diz respeito à região e a todas as cidades, e está ganhando visibilidade crescente na agenda política subnacional, nacional, regional e global, enquadrada em um processo de globalização dos sistemas de informação e das cadeias de valor.

18. O Marco mencionado estava pendente de aprovação no momento da publicação deste documento.

É por isso que o BID, na qualidade de parceiro estratégico, procura apoiar os países da região para enfrentar o novo desafio da cibersegurança urbana.

O Banco possui alianças estratégicas com os governos mais avançados em questões digitais, o que inclui a cibersegurança, como os do Canadá, Espanha, Estônia, Israel, Reino Unido e República da Coréia, bem como com parceiros-chave no meio acadêmico, no setor privado e em organismos de desenvolvimento, facilitando o acesso rápido e o compartilhamento de conhecimentos.

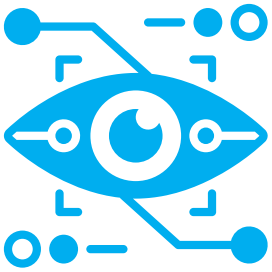

Scott Graham

Além disso, a equipe técnica do BID colabora com as equipes dos governos beneficiários e apoia a transformação digital adaptada à realidade de cada país, região metropolitana ou município.

O Banco conta com uma equipe dedicada a oferecer apoio aos países da ALC em questões de cibersegurança, que faz parte da Divisão de Inovação para Servir o Cidadão (IFD/ICS). No seu cluster de **Dados e Governo Digital** são concebidos projetos para reforçar a cibersegurança no nível nacional ou as capacidades de cibersegurança em setores dos quais os cidadãos dependem, como transporte, saúde, serviços financeiros, segurança do cidadão e governo digital, entre outros. Além disso, é prestado apoio na formulação de políticas públicas de cibersegurança, formação de profissionais e geração e intercâmbio de conhecimentos. Entre os estudos publicados pela equipe, destaca-se o Relatório Cibersegurança 2020: Riscos, Avanços e o Caminho a Seguir na América Latina e Caribe, realizado em colaboração com a OEA e que reúne as políticas e práticas de cibersegurança dos países da região, sua maturidade digital e as falhas e oportunidades para ação nesse campo.

No nível subnacional, as cidades da região registraram crescimento populacional acelerado nas últimas décadas, com o que a transformação digital e a adoção de tecnologia para o fornecimento de bens e serviços públicos adquiriu maior relevância.

Como resultado, a cibersegurança municipal e urbana transformou-se rapidamente em uma questão fundamental, que precisa ser abordada de forma preventiva.



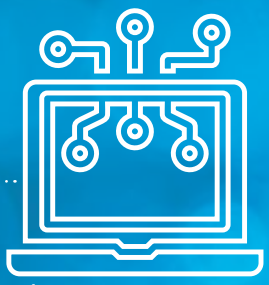
Nesta área, o Grupo Temático **Cidades Inteligentes e Dados Cívicos**, da Divisão de Habitação e Desenvolvimento Urbano do Banco (CSD/HUD), presta apoio para a transformação das cidades em direção a um modelo de cidades inteligentes e digitalmente seguras. No nível local, a importância da cibersegurança aumenta conforme se recorre cada vez mais à tecnologia para a prestação de serviços e a gestão da infraestrutura física e digital.

Para reduzir a discrepância de conhecimentos sobre transformação digital, o BID desenvolveu estudos, projetos piloto e ferramentas de autoavaliação em cibersegurança em setores como energia e saúde, aos quais se acrescenta agora a área específica das cidades (https://www.iadb.org/cibereval). Essa ferramenta ajudará tanto a compreender o nível de prevenção e preparação para ataques cibernéticos quanto a definir futuras iniciativas de capacitação nas quais o BID possa fornecer apoio para reforçar a cibersegurança urbana.

Esperamos que este Guia de cibersegurança para cidades inteligentes seja o ponto de partida para entender melhor a cibersegurança, bem como os riscos e possíveis impactos, além de difundir recomendações para transformar as 17.000 cidades da região em cidades mais inteligentes e ciberseguras.

Sung Jin Cho

Conclusões



As ameaças cibernéticas estão às portas de todas as cidades, à espreita de qualquer vulnerabilidade tecnológica ou humana. A cibersegurança total não existe, porém são muitas as medidas que podem ser adotadas em cada cidade para conseguir a maior proteção possível. É verdade que isso exige recursos, mas, como tudo na vida, o que é particularmente necessário é a vontade inequívoca e o compromisso claro por parte dos gestores e servidores municipais, bem como das empresas que colaboram nesse campo.

Com este guia, não apenas é possível conhecer o problema, mas também começar a enfrentá-lo de imediato, de acordo com as capacidades e a posição ocupada na cidade. Para que o ambiente seja seguro e digitalmente resiliente, ou seja, para garantir a continuidade da prestação de serviços urbanos, é necessário conhecer o ambiente a ser protegido, o ecossistema e os atores envolvidos. Deve ser entendido que é preciso gerir os riscos associados a cada serviço. A partir daí, é uma questão de planejar as atividades, analisar a colaboração entre as partes, buscar a formação e a capacitação contínuas, obter os recursos necessários e determinar os passos concretos a serem dados. É preciso ser proativo, ter uma clara vontade de cooperar com os atores envolvidos, praticar e treinar e capacitar-se. Vale a pena.

Sander Weeteling

Yiran Ding

Referências

AEC (Asociación Española para la Calidad). 2011. Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes. Madri: AEC. Disponível em: https://www.aec.es/conocimiento/documento/dictamen-13-2011-sobre-los-servicios-de-geolocalizacion-en-los-dispositivos-moviles-inteligentes/.

AEPD (Agencia Española de Protección de Datos). 2017. Código de buenas prácticas en protección de datos para proyectos Big Data. Madri: AEPD. Disponível em: https://www.aepd.es/es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf.

------. 2018. Guía para Administraciones Locales. Madri: AEPD. Disponível em: https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf.

------. 2019a. Guía Orientaciones e garantías en los procedimientos de anonimización de datos personales. Madri: AEPD. Disponível em: https://www.aepd.es/es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf.

------. 2019b. Directrices para la elaboración de contratos entre responsables e encargados del tratamiento. Madri: AEPD. Disponível em: https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf.

------. 2020a. Adecuación al RGPD de tratamientos que incorporan inteligencia artificial: una introducción. Madri: AEPD. Disponível em: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf.

------. 2020b. Tecnologías e Protección de Datos en las AAPP. Madri: AEPD. Disponível em: https://www.aepd.es/es/media/guias/guia-tecnologias-admin-digital.pdf.

------. 2020c. Webinario AEPD "Smart Cities: Más allá de la seguridad, la privacidad de los ciudadanos". Madri: AEPD. Disponível em: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/webinario-smart-cities.

------. 2021. Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD. Madri: AEPD. Disponível em: https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf.

Agrafiotis, I. et al. 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, Vol. 4(1), tyy006. Disponível em: https://doi.org/10.1093/cybsec/tyy006.

Alianza Global de Ciudades Inteligentes del G-20. 2020. Política modelo. Política de rendición de cuentas de ciberseguridad. Tóquio: World Economic Forum Centre for the Fourth Industrial Revolution Japan. Disponível em: http://globalsmartcitiesalliance.org/wp-content/uploads/2020/12/Cyber-accountability-v1.2-ESP.pdf.

Alibasic, A., R. Al Junaibi, Z. Aung, W. Woon e M. I. Omar. 2017. Cybersecurity for Smart Cities: A Brief Review. Lecture Notes in Computer Science, 10097: 22-30. Disponível em: https://www.researchgate.net/publication/312528431_Cybersecurity_for_Smart_Cities_A_Brief_Review.

Barrero, V. 2018. Estado de preparación en ciberseguridad del sector eléctrico en América Latina. Diagnóstico, recomendaciones e guía de buenas prácticas. Washington, D.C.: BID, Comisión de Integración Energética de la Comunidad, Govertis. Disponível em: https://publications.iadb.org/publications/spanish/document/Estado-de-preparacion-en-ciberseguridad-del-sector-electrico-en-America-Latina.pdf.

BID (Banco Interamericano de Desenvolvimento) e OEA (Organização dos Estados Americanos). 2020. Reporte ciberseguridad 2020: riesgos, avances e el camino a seguir en América Latina e el Caribe. Washington, D.C.: BID. Disponível em: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

Biderman, C. et al. 2021. Big Data para o desenvolvimento urbano sustentável. Washington, D.C.: BID. https://publications.iadb.org/pt/big-data-para-o-desenvolvimento-urbano-sustentavel.

BlueVoyant. 2020. State and local government security report. https://www.bluevoyant.com/wp-content/uploads/2020/11/BlueVoyant-State-and-Local-Government-Report-26th-August-2020-FINAL.pdf.

Bouskela, M. et al. 2016. Caminho para as Smart Cities Da Gestão Tradicional para a Cidade Inteligente. Washington, D.C.: BID. Disponível em: https://publications.iadb.org/publications/portuguese/document/Caminho-para-as-smart-cities-Da-gest%C3%A3o-tradicional-para-a-cidade-inteligente.pdf.

CCN (Centro Criptológico Nacional). 2020. Guía de Seguridad de las TIC. CCN-STIC 803. ENS. Valoración de los sistemas. Madri: Ministerio de Defensa. Disponível em: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html.

Cerdeira, P. et al. 2020. Políticas públicas orientadas por dados: Os caminhos possíveis para governos locais. Washington, D.C.: BID. Disponível em: https://publications.iadb.org/publications/portuguese/document/Politicas-publicas-orientadas-por-dados-Os-caminhos-possiveis-para-governos-locais.pdf, http://dx.doi.org/10.18235/0002727.

Cerrudo, C., M. A. Asbini e B. Russell. 2015. Cyber Security Guidelines for Smart City Technology Adoption. Securing Smart Cities, pp. 1-17. Cloud Security Alliance (CSA). Disponível em: https://securingsmartcities.org/wp-content/uploads/2016/03/Guidlines_for_Safe_Smart_Cities-1.pdf.

Crowdstrike. 2021. Global Threat Report. Disponível em: https://www.crowdstrike.com/resources/reports/global-threat-report-es/.

CSIS (Center for Strategic & International Studies). 2021. Significant Cyber Incidents since 2006. Washington, D.C.: CSIS. Disponível em: https://csis-website-prod.s3.amazonaws.com/s3fs-public/210804_Significant_Cyber_Events.pdf?bzKYK94rq5_3lrbYVK4fcL0rmkNq6lNI.

DHS/OCIA (Department of Homeland Security's Office of Cyber and Infrastructure Analysis). 2015. The future of smart cities: cyber-physical infrastructure risk. Washington, D.C.: DHA/OCIA. Disponível em: https://us-cert.cisa.gov/ics/Future-Smart-Cities-Cyber-Physical-Infrastructure-Risk.

ECSO (European Cyber Security Organisation). 2018. Smart cities and smart buildings sector report. Cyber security for the smart cities sector, WG3 Sectoral Demand. Bruselas: ECSO. Disponível em: https://ecs-org.eu/documents/publications/5fdb27182b472.pdf.

Efthymiopoulos, M-P. 2016. Cyber-security in smart cities: The case of Dubai. Journal of Innovation and Entrepreneurship, 5(11). Disponível em: DOI 10.1186/s13731-016-0036-x.

Enerlis, Ernst and Young, Ferrovial e Madri Network. 2012. Libro Blanco Smart Cities. 1.ª edição. Disponível em: http://www.innopro.es/pdfs/libro_blanco_smart_cities.pdf.

ENISA (Agência da União Europeia para a Segurança das Redes e da Informação). 2014. Secure ICT Procurement in Electronic Communications. Analysis and recommendations for procuring ICT securely in the Electronic Communications Sector. Heraclión: ENISA. Disponível em: https://www.enisa.europa.eu/publications/secure-ict-procurement-in-electronic-communications/at_download/fullReport.

------. 2015. Cyber security for Smart Cities. An architecture model for public transport. Heraclión: ENISA. Disponível em: https://www.enisa.europa.eu/publications/smart-cities-architecture-model.

------. 2020. Directrices sobre contratación para la ciberseguridad en los hospitales. Prácticas recomendadas para la seguridad de los servicios sanitarios. Heraclión: ENISA. Disponível em: https://www.enisa.europa.eu/publications/report-files/translation-procurement-guidelines-for-cybersecurity-in-hospitals/procurement-guidelines-full-version-es.pdf.

Eurocities. 2016. EUROCITIES statement on the contractual public-private partnership on cybersecurity. Bruselas: Eurocities. Disponível em: http://nws.eurocities.eu/MediaShell/media/EUROCITIES_cybersecurity_statement.pdf.

FEM (Fórum Econômico Mundial). 2021. Whitepaper, Governing Smart Cities: Policy Benchmarks for Ethical and Responsible Smart City Development. Ginebra: FEM e Deloitte. Disponível em: https://www.weforum.org/whitepapers/governing-smart-cities-policy-benchmarks-for-ethical-and-responsible-smart-city-development.

Forrest, C. 2019. Vendor selection: what needs to be in a good policy. En: ZDNet-TechRepúblic, A winning strategy for cybersecurity. San Francisco, CA: CBS Interactive Inc. Disponível em: http://book.itep.ru/depository/security/surveys/SF_feb2019_cybersec.pdf.

Gagliordi, N. 2019. Electronic communications: what needs to be in a good policy. En: ZDNet-TechRepúblic, A winning strategy for cybersecurity. San Francisco, CA: CBS Interactive Inc. Disponível em: http://book.itep.ru/depository/security/surveys/SF_feb2019_cybersec.pdf.

García, M., D. Forscey e T. Blute. 2017. Beyond the Network: A Holistic Perspective on State Cybersecurity Governance. Nebraska Law Review, 96 (2).

Gómez de Ágreda, Á. 2020. Ciberseguridad en ciudades. En: Las ciudades: agentes críticos para una transformación sostenible del mundo. Cuaderno de Estrategia 206. Madri: Instituto Español de Asuntos Estratégicos. Disponível em: http://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2020/Cuaderno_206.html.

ICO (Information Commisioner Office). s.f. Anonymisation: managing data protection risk code of practice. Wilmslow: ICO. Disponível em: https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf.

INCIBE (Instituto Nacional de Ciberseguridad). 2016. CEO, CISO, CIO... ¿Roles en ciberseguridad? León, Espanha: INCIBE. Disponível em: https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad.

INCIBE-OSI (Oficina de Seguridad del Internauta). s.f. Guía de ciberataques. León, Espanha: INCIBE. Disponível em: https://www.osi.es/es/guia-ciberataques.

Information System Authority. 2021. Three-level Baseline Security System ISKE. Tallin: República da Estônia. Disponível em: https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html.

Interpol (Organização Internacional de Polícia Criminal). 2020. Panorama mundial de la ciberamenaza relacionada con la COVID-19. Madri: Interpol. Disponível em: https://www.interpol.int/es/Delitos/Ciberdelincuencia/Ciberamenazas-relacionadas-con-la-COVID-19.

IOActive. 2018. Smart Cities Cyber Security Worries. Seattle, WA: IOActive. https://ioactive.com/wp-content/uploads/2018/10/IOActive-SmartCities-cybersecurity-worries.pdf.

ISO (Organização Internacional de Normalização). 2012. ISO/IEC 27032:2012: Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad. Genebra: ISO. Disponível em: https://www.iso.org/standard/44375.html.

------. 2018. SO/IEC 27005: Gestión de riesgos de la seguridad la información. Genebra: ISO. Disponível em: https://www.iso.org/standard/75281.html.

Kalinin, M. et al. 2021. Cybersecurity Risk Assessment in Smart City Infrastructures. Machines, 9, 78. Disponível em: https://doi.org/10.3390/machines9040078.

La French Tech. 2019. C'est quoi La French Tech Rennes St Malo? Rennes St Malo: La French Tech. Disponível em: https://lafrenchtech-rennes.fr/.

Mantelero, A. 2017. From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era. En: L. Taylor, L. Floridi e B. van der Sloot (eds.), Group privacy: new challenges of data technologies. Dordrecht: Springer. Disponível em: https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf.

Martín, E. 2016. Smart Cities: El valor de construir ciudades inteligentes. Revista TELOS, 105. Disponível em: https://telos.fundaciontelefonica.com/archivo/numero105/el-valor-de-construir-ciudades-inteligentes-con-ciberseguridad/.

MIAC (Ministry of Internal Affairs and Communications). 2020. Smart City Security Guidelines. Tokio: MIAC. Disponível em: https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/Smart_City_Security_Guideline_ver1.0.pdf.

MINTIC (Ministerio de Tecnologías de la Información e las Comunicaciones). 2021. Modelo de Seguridad e Privacidad de la Información, v. 4.0. Bogotá: MINTIC. Disponível em: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/.

Muñoz, M. et al. 2018. Guía de Buenas Prácticas sobre Smart City para pequeños e medianos municipios. Granada: Diputación de Granada, Red Granadina de Municipios hacia la Sostenibilidad (GRAMAS). Disponível em: https://www.dipgra.es/uploaddoc/areas/349/SMARTCITY.pdf.

NCSC (National Counterintelligence and Security Center). 2021. Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective. Londres: NCSC. https://www.dni.gov/files/NCSC/documents/news/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021.pdf.

New America, N. Cohen e B. Nussbaum. 2018. Cybersecurity for the States: Lessons from Across America. Washington, D.C.: Cybersecurity Initiative, New America. Disponível em: https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-states-lessons-across-america/.

------. 2019. Smart is Not Enough. How to ensure the technologies of the future don't break our cities (and us with them). Washington, D.C.: Cybersecurity Initiative, New America. Disponível em: https://www.jstor.org/stable/resrep19969.1.

NIST (Instituto Nacional de Estándares e Tecnología). 2008. Guide for Mapping Types of Information and Information Systems to Security Categories. Special Publication 800-60 Volume I, Revision 1. Gaithersburg, MD: NIST. Disponível em: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152106.

------. 2019. Smart and Secure Cities and Communities Challenge (SC3), GCTC-SC3 Cybersecurity and Privacy Advisory Committee Guidebook, Global City Teams Challenge 2019. Gaithersburg, MD: NIST. Disponível em: https://www.nist.gov/publications/2019-global-city-teams-challenge-smart-and-secure-cities-and-communities-challenge-expo.

OCDE (Organización para la Cooperación e el Desarrollo Económicos). 2015. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. París: OCDE. Disponível em: http://dx.doi.org/10.1787/9789264245471-en.

OEA (Organização dos Estados Americanos). 2019. Clasificación de datos. White paper series. Washington, D.C.: OEA. Disponível em: https://www.oas.org/es/sms/cicte/docs/ESP-Clasificacion-de-Datos.pdf.

OSPI (Observatorio del Sector Público). 2017. Ciberseguridad en el sector público. Documento de conclusiones. Disponível em: https://www.ospi.es/export/sites/ospi/documents/informes/Informe_ciberseguridad.pdf.

Pandey, P. et al. 2020. Making smart cities cybersecure. Ways to address distinct risks in an increasingly connected urban future. Deloitte Insights. Disponível em: https://www2.deloitte.com/us/en/insights/focus/smart-city/making-smart-cities-cyber-secure.html.

PwC. 2021. Global Digital Trust Insights Survey 2021. Cybersecurity comes of age. Londres: PwC. Disponível em: https://www.pwc.com/gx/en/issues/cybersecurity/digital-trust-insights-2021.html.

Ranchordás S. e C. Goanta. 2020. The New City Regulators: Platform and Public Values in Smart and Sharing Cities. Computer Law & Security Review, 36. Disponível em: https://doi.org/10.1016/j.clsr.2019.105375.

Razavi, A., S. Moschoyiannis e P. Krause. 2009. An open digital environment to support business ecosystems. Peer-To-Peer Networking and Applications, 2(4): 367-397. Disponível em: DOI:10.1007/s12083-009-0039-5.

Rea-Guaman, Á. M., I. S. Sánchez-García, T. San Feliu Gilabert e J. A. Calvo-Manzano Villalón. 201). Modelos de madurez en ciberseguridad: una revisión sistemática. En: 12ª Conferencia Ibéricas de Sistemas e Tecnologías de la Información, 21-24 de junho de 2017, Lisboa, Portugal, pp. 284-289.

Salvador, C. 2021. Inteligencia artificial e gobernanza de datos en la administración pública: sentando las bases para su integración a nivel corporativo. En: R. Carles (coord.), Repensando la Administración Pública. Administración digital e innovación pública. Madri: INAP. Disponível em: https://www.libreriavirtuali.com/inicio/Administraci%C3%B3n-digital-e-innovaci%C3%B3n-p%C3%BAblica-Repensando-la-Administraci%C3%B3n-P%C3%BAblica-EBOOK-p306540049.

Shacklett, M. 2019. 10 ways to develop cybersecurity policies and best practices. En: ZDNet-TechRepúblic, A winning strategy for cybersecurity. San Francisco, CA: CBS Interactive Inc. Disponível em: http://book.itep.ru/depository/security/surveys/SF_feb2019_cybersec.pdf.

Soare, S. e J. Burton. 2020. Smart Cities, Cyber Warfare and Social Disorder. CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence. Disponível em: https://ccdcoe.org/uploads/2020/12/6-Smart-Cities-Cyber-Warfare-and-Social-Disorder_ebook.pdf.

Stilgherrian. 2019. Security training is useless unless it changes behaviours. ZDNet-TechRepúblic, A winning strategy for cybersecurity. San Francisco, CA: CBS Interactive Inc. Disponível em: http://book.itep.ru/depository/security/surveys/SF_feb2019_cybersec.pdf.

Townsend, A. e P. Zambrano-Barragán. 2019. Big Urban Data. A Strategic Guide for Cities. Washington, D.C.: BID. Disponível em: https://publications.iadb.org/publications/spanish/document/BIG_Data_urbana_Una_gu%C3%ADa_estrat%C3%A9gica_para_ciudades.pdf.

Trapenberg, F. et al. 2021. The Cybersecurity Risks of Smart City Technologies, What Do the Experts Think? UC Berkeley, CLTC White Paper Series. Disponível em: https://cltc.berkeley.edu/2021/03/16/smart-cities/.

UIT (União Internacional de Telecomunicações). 2008. Cláusula 3.2.5 de la Rec. UIT-T X.1205 (04/2008). Genebra: UIT. Disponível em: https://handle.itu.int/11.1002/1000/9136.

UNE (Asociación Española de Normalización). 2021. Comité CNT 178: Ciudades inteligentes. Madri: UNE. Disponível em: https://www.une.org/encuentra-tu-norma/comites-tecnicos-de-normalizacion/comite?c=CTN%20178.

Guia de cibersegurança para cidades inteligentes

AUTORES: Lorenzo **Cotino**
Marco **Sánchez**

EDITORES: Mauricio **Bouskela**
Gilberto **Chona**
Ariel **Nowersztern**
Patricio **Zambrano-Barragán**
Isabelle **Zapparoli**

BID