ARTIGO · JOTA_IMPORT

Segurança da informação e IoT no Brasil: prioridades, modelos e alternativas

Autor(a): Mateus Piva Adami
Publicado em: 06 de março de 2018
Publicação: jota_import
Link JurisTube: https://juristube.com.br/colunistas/mateus-piva-adami/seguranca-da-informacao-e-iot-no-brasil-prioridades-modelos-e-alternativas
Fonte original: https://www.jota.info/opiniao-e-analise/artigos/seguranca-da-informacao-e-iot-no-brasil-prioridades-modelos-e-alternativas
Identificador citável: juristube.com.br/colunistas/mateus-piva-adami/seguranca-da-informacao-e-iot-no-brasil-prioridades-modelos-e-alternativas#ep-77eea092

Resumo

País deve definir uma estratégia de segurança da informação, cujo norte seja a atuação multissetorial

Texto integral

Como parte da série sobre o direito e a Internet das Coisas (‘ internet of things ’ ou ‘IoT’), em parceria com o JOTA , este artigo discute os rumos do modelo institucional brasileiro para o tema de segurança da informação. 1 A IoT é caracterizada pela adoção em massa de dispositivos e sensores de baixo custo, que em muitas vezes não atendem a padrões de segurança mínimos, conectados a redes por vezes inseguras. Somada à natureza “sem fronteiras” de incidentes e a possibilidade para a expansão de vulnerabilidades, entra em pauta a preocupação com a segurança de redes e dispositivos. +JOTA: O Direito da Internet das Coisas – desafios e perspectivas de IoT no Brasil O momento é oportuno. Raramente um dia se passa sem que haja notícias e estatísticas sobre novos incidentes maliciosos a dispositivos e redes, danos causados e investimentos considerados necessários para proteção contra novas falhas ou ataques. Dados demonstram que o Brasil foi o segundo país que mais sofreu perdas financeiras com crimes cibernéticos em 2017 (em torno de US$ 22 bilhões), sendo superado apenas pela China. 2 Cerca de 62 milhões de brasileiros foram afetados no período por incidentes como hacking (acesso não autorizado a dispositivos) e ataques distribuídos de negação de serviço (nos quais o tráfego de dados decorrente de uma imensidão de dispositivos é direcionado a um servidor, a fim de sobrecarrega-lo). 3 Com o avanço da adoção de dispositivos e serviços IoT na vida doméstica e em setores como saúde, rural e indústrias, a questão se torna ainda mais imediata e amplia exponencialmente os valores envolvidos – em termos de prejuízos e medidas para mitigação de riscos. +JOTA: Neutralidade da rede e Internet das Coisas no Brasil: uma relação harmônica Panorama internacional . Face a esse cenário, uma primeira preocupação tem a ver com o modelo adotado pelo Brasil para a cooperação com outros países na proteção contra crimes cibernéticos, notadamente considerando seu caráter transnacional. Atualmente, o país opta pela assinatura de 'Acordos de Troca e Proteção Mútua de Informações Classificadas ' com países estratégicos. 4 Esses acordos permitem o auxílio direto entre um país e outro e a troca de experiências institucionais e de melhores práticas. Ainda assim, é tempo para aprimorarmos os mecanismos atuais para a prevenção e tratamento de incidentes com outros países, equilibrando as medidas previstas para cooperação policial e o respeito aos direitos

fundamentais do indivíduo. Uma possibilidade viável é justamente buscar adotar um maior número de Acordos de Troca e Proteção Mútua de Informações Classificadas. Por um lado, esse modelo apresenta desafios, como a dificuldade em acompanhar a troca de dados simultânea entre diversos países - o que seria impulsionado pela IoT. Por outro, a busca por novos acordos pode enriquecer o ordenamento jurídico interno brasileiro, além de assegurar que o mesmo permaneça pari passu com o que há de mais contemporâneo em termos de arcabouço normativo de cibersegurança. De forma complementar, o Brasil pode se aproximar da liderança regional exercida pela Organização dos Estados Americanos (OEA) e dos seus programas de segurança cibernética, de modo a fortalecer a cooperação regional e internacional no tópico. Outro movimento importante para a adoção de melhores práticas internacionais é garantir que o País acompanhe as iniciativas de definição de standards internacionais, bem como de autorregulação ou de regulação híbrida com relação a temas de cibersegurança. Incentivar que fornecedores de equipamentos, software e outros insumos de IoT estejam certificados por organizações internacionais (tais como a IEEE) é um caminho efetivo, de baixo custo institucional e capaz de produzir resultados imediatos. +JOTA: Qual o conceito de M2M e por que isso importa para o desenvolvimento de IoT? Arranjo institucional . Já no âmbito interno, hoje não é possível identificar uma estrutura de governança definida na Administração Pública Federal em relação à segurança da informação, o que representa um gargalo na adoção e coordenação de medidas. É fundamental que o País defina uma estratégia de segurança da informação, cujo norte seja a atuação multissetorial, isto é, a cooperação entre os diversos setores relevantes, como o Poder Público, setor privado, academia, comunidade técnica e científica, além da sociedade civil. Há alguns modelos institucionais possíveis, como a criação de um conselho permanente, que poderia atuar em caráter consultivo para a elaboração de políticas nacionais e como um hub de articulação entre diferentes setores. Este conselho poderia ser composto por estrutura adequada para a proteção da segurança da informação no contexto da adoção e desenvolvimento de IoT, e para a coordenação da cooperação entre os órgãos e entidades do Poder Público. É o modelo escolhido pela Holanda, com o Nationaal Cyber Security Centrum . O órgão é responsável por supervisionar a estratégia nacional em cibersegurança e é composto por membros do governo, indústria, comunidade científica, setor público e iniciativa privada. 5 Qualquer que seja o modelo adotado, o fundamental é criar ou designar um órgão competente que atue para a criação de um ambiente de confiança entre o Poder Público e a iniciativa privada, a sociedade civil e a academia. Trata-se de passo essencial para tratar de temas de cibersegurança. +JOTA: A necessidade de investimentos na infraestrutura de telecomunicações Infraestruturas críticas . Outro aspecto estratégico no tema de segurança da informação e IoT diz respeito ao grau de segurança de infraestruturas consideradas críticas, como redes de saneamento básico e energia elétrica. 6 Com a adoção em massa de soluções de IoT, uma falha de segurança ou ataque malicioso aos sistemas envolvidos na prestação de serviços essenciais traria um impacto social tremendo, o que exige robustez redobrada em medidas de segurança da informação. 7 Embora já haja atualmente iniciativas no âmbito da Administração Federal, ligadas ao Gabinete de Segurança Institucional da Presidência da República, deve haver engajamento na coordenação de esforços e no estabelecimento de parcerias com, por exemplo, centros técnicos. 8 Isso se deve em função do dinamismo associado a esse tipo de risco. Como exemplo da relevância da cooperação entre diferentes atores, em caso recente, um software malicioso infectou os sistemas de três subestações de distribuição de energia elétrica em país do leste europeu, deixando centenas de milhares de cidadãos sem energia elétrica até ser detectado por pesquisadores e corrigido. 9 Uma possibilidade imediata é a criação de roadmaps por ministérios e órgãos públicos para a prevenção de incidentes

de segurança, detecção, resposta e gestão de crises. Outro ponto é a possibilidade de agências reguladoras exigirem que concessionárias respeitem aspectos mínimos de segurança da informação. +JOTA: Principais desafios tributários do ambiente de Internet das Coisas Próximos passos . O desenvolvimento da Internet das Coisas no Brasil deve ser acompanhado de medidas concretas por parte do Poder Público para garantir a construção de um ambiente de confiança e o avanço de um ambiente institucional adequado para a segurança da informação. Um primeiro passo nesse sentido é definir uma estratégia clara baseada na cooperação entre o Estado, a sociedade, a iniciativa privada e os demais setores – o que, em nosso entendimento, passa pelos elementos aqui tratados. No próximo artigo da série sobre direito e Internet das Coisas, continuamos o debate com uma contribuição sobre o arranjo institucional para a proteção de dados no Brasil. Até lá! ---------- 1 ■ Este é o sexto artigo resultante do documento elaborado pelo escritório Pereira Neto, Macedo no Estudo Técnico “Internet das Coisas: um plano de ação para o brasil”, apoiado pelo BNDES em parceria com o MCTIC. Para conferir mais sobre o estudo e ver os relatórios já publicados, acesse: https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil 2 ■ Conforme disponível em https://goo.gl/1dmeDq . 3 ■ Para mais informações sobre o ecossistema de ataques a dispositivos IoT, sugerimos consulta à Cartilha de Segurança para Internet, v.4.0, publicada pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (“CERT.br”). Disponível em https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf . Para mais dados sobre os ataques sofridos no Brasil em 2017, acesse http://cio.com.br/noticias/2018/01/31/brasil-sofreu-264-9-mil-ataques-ddos-em-2017-35-gerados-no-proprio-pais/ . 4 ■ O Brasil possui uma série de acordos bilaterais em vigor com esse fim, com países como China, Canadá, Cuba, México, França, Nigéria, Panamá, Suriname, EUA, Colômbia, Peru, Portugal, Espanha, Rússia, Itália, Israel, Reino Unido e Suécia. Para detalhes sobre as diligências permitidas e os requisitos necessários para a concessão de assistência, cabe referência à Cartilha de Cooperação Jurídica Internacional em Matéria Penal, publicada pelo Ministério da Justiça e disponível em https://goo.gl/X9CmLs . 5 ■ Para mais informações, ver https://www.ncsc.nl/english. 6 ■ Segundo a Portaria nº 2/2008 do GSI/PR, são “infraestruturas críticas” as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional. Destas, são infraestruturas críticas prioritárias as áreas de energia, água, transporte, telecomunicações e finanças. Disponível em http://contadores.cnt.br/legislacoes/portaria-gsipr-no-2-de-8-de-fevereiro-de-2008.html . 7 ■ Em exemplo menos prejudicial, mas ainda assim preocupante, um malware foi detectado em rede de distribuição de água na Europa em fevereiro de 2018, com o objetivo de utilizar a sua capacidade de processamento para a mineração de criptomoedas. Portanto, tal ataque não atingiu algum aspecto central da prestação do serviço público. Ver http://www.eweek.com/security/water-utility-in-europe-hit-by-cryptocurrency-malware-mining-attack . 8 ■ O Decreto nº 7.009/2009 tornou o tema uma atribuição da Câmara de Relações Exteriores e Defesa Nacional (“CREDEN”), presidida pelo Ministro-Chefe do GSI/PR. Ainda, o Departamento de Segurança da Informação e Comunicações (“DSIC”), também ligado ao GSI/PR, publicou o Guia de Referência Para a Segurança das Infraestruturas Críticas da Informação ainda em 2010, que se mantém como referência para modelo institucional no tema. Disponível em http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf . 9 ■ Para mais informações a respeito, ver https://arstechnica.com/information-technology/2016/01/first-known-hacker-caused-pow

er-outage-signals-troubling-escalation/?comments=1 .

Como citar este documento

As citações abaixo seguem os padrões ABNT NBR 6023:2018, APA 7ª edição, Chicago Author-Date (17ª ed.) e BibTeX (LaTeX). Copie o formato exigido pelo periódico ou gerenciador bibliográfico (Zotero, Mendeley, EndNote).

ABNT (NBR 6023:2018)

ADAMI, Mateus Piva. Segurança da informação e IoT no Brasil: prioridades, modelos e alternativas. jota_import, 6 mar. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/seguranca-da-informacao-e-iot-no-brasil-prioridades-modelos-e-alternativas. Acesso via: JurisTube — Acervo Digital de Direito. Disponível em: https://juristube.com.br/colunistas/mateus-piva-adami/seguranca-da-informacao-e-iot-no-brasil-prioridades-modelos-e-alternativas. Acesso em: 26 ago. 2026.

APA 7ª edição

Adami, M. P. (2018, March 6). Segurança da informação e IoT no Brasil: prioridades, modelos e alternativas. *jota_import*. https://www.jota.info/opiniao-e-analise/artigos/seguranca-da-informacao-e-iot-no-brasil-prioridades-modelos-e-alternativas

Chicago Author-Date (17ª ed.)

ADAMI, Mateus Piva. 2018. “Segurança da informação e IoT no Brasil: prioridades, modelos e alternativas.” *jota_import*, March 06. https://www.jota.info/opiniao-e-analise/artigos/seguranca-da-informacao-e-iot-no-brasil-prioridades-modelos-e-alternativas

BibTeX

```
@article{mateus-piva-adami-seguran-a-da-informa-o-e-iot-no-brasil-p-2018,
author = {Adami, Mateus Piva},
title = {Segurança da informação e IoT no Brasil: prioridades, modelos e alternativas},
journal = {jota_import},
year = {2018},
url = {https://www.jota.info/opiniao-e-analise/artigos/seguranca-da-informacao-e-iot-no-brasil-prioridades-modelos-e-alternativas},
urldate = {2018-03-06}
}
```


JurisTube — Acervo Digital de Direito
https://juristube.com.br/colunistas/mateus-piva-adami/seguranca-da-informacao-e-iot-no-brasil-prioridades-modelos-e-alternativas
PDF gerado em 2026-08-26 19:09 UTC