Internet of Things (IoT) aplicada para resolução de desafios na Administração Pública

Conexão, Segurança e Privacidade na IoT

Módulo 2

Gestão da Comunicação e do Conhecimento.

EV.G

Enap

Fundação Escola Nacional de Administração Pública

Diretoria de Desenvolvimento Profissional

Conteudista
Taiser Barros (conteudista, 2022);
Diretoria de Desenvolvimento Profissional.

Enap, 2022
Fundação Escola Nacional de Administração Pública
Diretoria de Desenvolvimento Profissional
SAIS - Área 2-A - 70610-900 — Brasília, DF

Sumário

Unidade 1: Redes, Dispositivos, Conexão e Segurança 4

1.1 Redes, Integrações e Padrões Utilizados na IoT 4

1.2 Modelos de Computação para Dispositivos na IoT 8

1.3 Coisas que podem se conectar 13

Referências 17

Unidade 2: Segurança e Privacidade 19

2.1 Segurança e Privacidade no uso da IoT 19

Referências 26

Módulo

2 Conexão, Segurança e Privacidade na IoT

Neste módulo, você verificará como ocorrem as conexões em uma rede de dispositivos IoT, focando nos tipos de redes disponíveis, modelos computacionais e nos dispositivos que podem se conectar a uma rede. Na sequência, será apresentado um estudo sobre questões de privacidade e segurança relacionados a redes de IoT, sendo este tópico fundamental para a compreensão de outros contextos, assim como a atual Lei Geral de Proteção de Dados (Lei nº 13.709/2018, também chamada de LGPD).

E então, você está pronto(a) para estudar os tópicos mencionados e ampliar seus conhecimentos sobre a IoT, os tipos de redes, conexões e segurança associados? Tome uma água, respire fundo e avance!

Unidade 1: Redes, Dispositivos, Conexão e Segurança

Objetivo de aprendizagem

Ao concluir esta unidade, você estará habilitado(a) a identificar as formas de conexão utilizadas na IoT.

1.1 Redes, Integrações e Padrões Utilizados na IoT

As informações aqui apresentadas sobre IoT possuem um caráter exploratório, buscando trazer a você, cursista, uma série de conceitos que possam habilitá-lo(a) a compreender a IoT em diferentes contextos. Alguns conceitos apresentados terão um teor mais genérico, enquanto outros focam em aspectos mais técnicos.

Especificamente neste tópico, em que serão abordadas as redes e padrões da IoT, é preciso trazer aspectos um pouco mais técnicos, como os protocolos de comunicação utilizados em IoT.

Para iniciar a análise, deve-se retomar a ideia de que a Internet das Coisas depende de uma conexão à internet e deve obedecer a um determinado padrão de conexão. Assim como qualquer outro dispositivo que se conecta à internet, exemplificando com os computadores e smartphones, será necessário que os dispositivos de uma rede IoT utilizem o protocolo IP (*Internet Protocol*).

A primeira versão do protocolo IP, o IPv4, foi criado em 1958 pela Defense Advanced Research Projects Agency (DARPA) e utiliza um endereçamento de 32 bits (SALAZAR; SILVESTRE, 2017).

> **A maioria dos computadores conectados à internet usa o protocolo IPv4, que é bastante confiável e flexível. No entanto, o crescimento exponencial da internet exigiu o surgimento de um novo protocolo, o IPv6, que é uma versão atualizada do IPv4, com as mesmas funcionalidades, mas sem as mesmas limitações (ABOUSALEM, ASHABRAWY, 2018).**

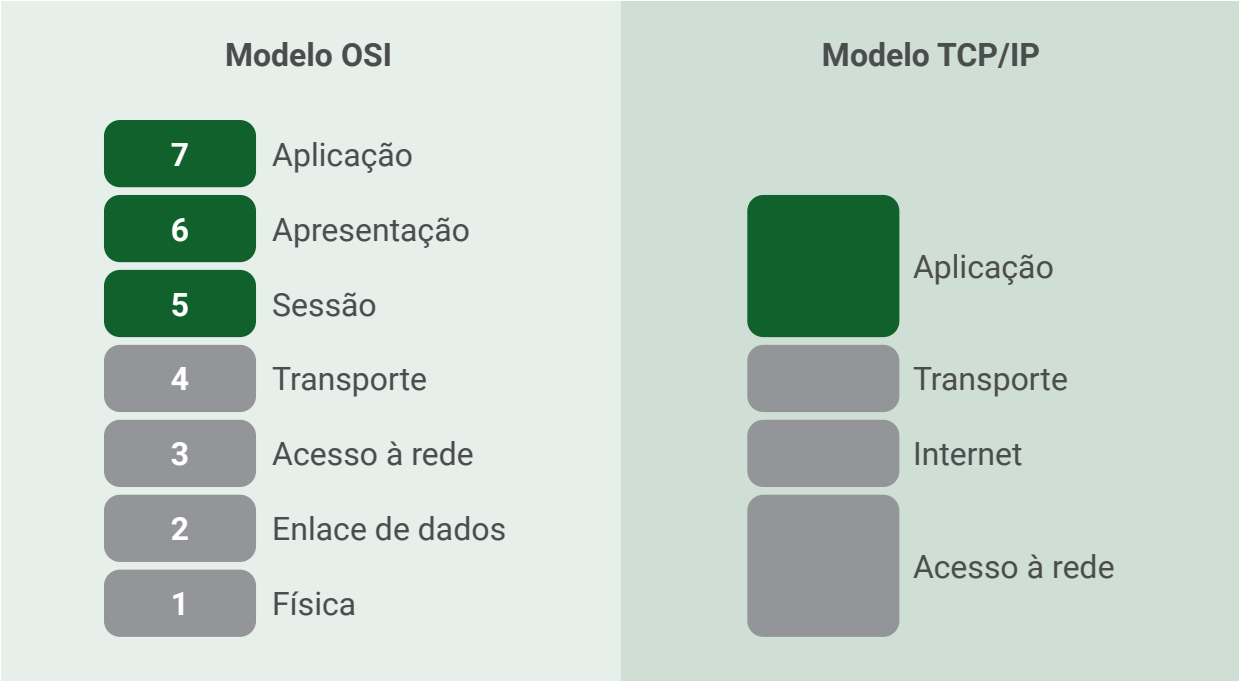
Convém destacar que o crescimento exponencial da internet se deve em grande parte ao surgimento da IoT, que conecta uma diversidade de "coisas" (objetos) à internet.

Uma ideia da ordem de grandeza dos números envolvidos nos protocolos iPv4 e IPv6 pode ser obtida pela análise do número de *bits* de endereçamento de cada protocolo. No sistema binário de numeração (que utiliza somente os dígitos 0 e 1), eleva-se a base 2 ao número de *bits* para saber a ordem de grandeza em decimal; assim, para o protocolo IPv4, o número de endereços disponibilizados é de $2^{32} = 4294967296$, ou aproximadamente 4.3 bilhões. Atualmente, 4.3 bilhões de endereços já é um número limitado frente ao número de dispositivos conectados.

Com relação ao protocolo IPv6, tem-se um endereçamento de 128 *bits*, que vai gerar um número da ordem de $8x10^{28}$ vezes o número de endereços do protocolo IPv4. Além do aumento significativo de endereços, Salazar e Silvestre (2017) destacam que o protocolo IPv6 possui administração mais simples, roteamento mais eficiente, autenticação embutida, suporte de privacidade, entre outras características.

SAIBA MAIS

O IP faz parte de uma teoria mais ampla e possui um modelo de implementação que considera as camadas de aplicação, transporte, rede e acesso à rede, similar ao modelo OSI/ISSO. Caso queira saber mais, assista ao vídeo, produzido pelo canal Redes Brasil clicando aqui.



Modelos OSI e TCP/IP.

Elaboração: CEPED/UFSC (2022). Adaptado de BNDES (2017)

Além do IP, que é padrão para diversas tecnologias se conectarem, existem os meios de comunicação, sendo os mais comuns o cabo de par trançado, cabo coaxial, fibra óptica e as conexões sem fio (BRITO *et al.*, 2019). Os autores trazem também uma lista de protocolos específicos para utilização com redes IoT, os quais foram compilados na tabela a seguir:

EMPRESA	DEFINIÇÃO
Bluetooth e Bluetooth Low Energy (BLE)	O *Bluetooth* foi popularizado em aplicações de transferência de dados e ligação de periféricos como fones de ouvidos, teclados e *mouses*. A variação BLE se caracteriza pelo baixo consumo de energia e é muito utilizada para aplicações que exigem um tempo de vida elevado de bateria. O BLE opera em uma banda de 2,4GHz, define 40 canais de radiofrequência e possui alcance limitado a 50 metros, sendo atualmente incompatível com o *Bluetooth* clássico.
ZigBee	Caracteriza-se pelos baixos consumo de energia, taxa de transmissão e custo de implementação. Com alcance máximo de 100 metros, pode atingir distâncias maiores repassando as informações pelos nós da rede em múltiplos saltos até alcançar o seu destino.
IPv6 Over Low Power Wireless Personal Area Networks (6LoWPAN)	Permite encapsular o protocolo IPv6 para redes sem fio de curto alcance. Os cabeçalhos do IPv6 devem ser fragmentados, compactados e reagrupados, fornecendo um endereço único para cada dispositivo IoT.
Long Range Wide Area Network (LoRaWAN)	Habilita redes IoT de longa distância, com acesso a dispositivos a uma distância de até 15 quilômetros, utilizando uma estação de rádio de longo alcance. Para atingir distâncias maiores, as frequências estão entre 433 e 915 MHz. Há diversas aplicações que podem ter grandes utilidades no futuro para serviços de tarifação, como água, energia e gás.
ESP-MESH	O avanço da IoT requer um número vasto de nós conectados à internet. No entanto, somente um número limitado de nós pode se conectar diretamente ao mesmo roteador. O protocolo ESP-MESH é uma das soluções para esse problema, disponibilizando uma rede *mesh* na qual cada dispositivo IoT se torna um nó, podendo estabelecer uma rede e encaminhar pacotes. Como resultado, um grande número de nós pode se conectar à internet sem melhoria no roteador.
ESP-NOW	É um tipo de protocolo de comunicação *wi-fi* sem conexão que não faz uso do protocolo TCP. É amplamente utilizado em ambientes de iluminação inteligente, sensores e atuadores, permitindo que vários dispositivos se comuniquem sem usar um roteador *wi-fi*. O protocolo é semelhante à conectividade sem fio de baixa potência de 2,4 GHz frequentemente implantada em mouses sem fio, sendo o pareamento entre dispositivos necessário antes da comunicação. Após o pareamento, a conexão é persistente e torna o protocolo mais eficiente e veloz na comunicação entre dispositivos IoT.
Message Queue Telemetry Transport (MQTT)	É um protocolo de mensagens simples e leve de publicação/assinatura projetado para dispositivos restritos e redes de baixa largura de banda, alta latência ou não confiáveis. Busca minimizar a largura de banda e os requisitos de recursos dos dispositivos. O protocolo é ideal para dispositivos conectados “máquina a máquina” e “Internet das Coisas” para aplicações móveis em que a largura de banda e bateria são essenciais.

Conforme você pôde observar, os diferentes protocolos disponíveis para serem implementados em redes IoT possuem características particulares que vão habilitar a utilização de um determinado protocolo para determinada aplicação.

Tomando como exemplo as características do protocolo LoRaWAN, que permite comunicação de dispositivos em distâncias de até 15 km entre "nós" conectados, é possível projetar uma série de aplicações. A própria questão de medição de consumo de água é um ótimo exemplo de aplicação, pois atualmente a medição de água é realizada em sua grande maioria por operadores humanos que efetuam a medida do consumo visitando residências e empreendimentos que consomem água de uma empresa.

Pensando na utilização de uma rede LoRaWAN, seria possível instalar medidores que transmitiriam os dados de consumo para uma central onde os dados seriam processados. Além da coleta dos dados, seria possível criar ainda análises de demanda de consumo em tempo real, permitindo que as companhias de fornecimento de água pudessem aprimorar os serviços prestados.

1.2 Modelos de Computação para Dispositivos na IoT

Conforme os conceitos discutidos sobre a Internet das Coisas, sabe-se que diversos dispositivos são conectados em uma rede IoT e, devido ao grande número de dispositivos que estão sendo conectados atualmente, o volume de dados a serem processados/armazenados é cada vez maior. Gerenciar todos estes dados exige diferentes estratégias de utilização de computadores (servidores).

> Alguns modelos de sistemas de computação utilizados atualmente e que buscam atender ao grande volume de dados gerado em redes IoT são a Computação na Borda ou Local (*Edge Computing*), Computação em Nuvem (*Cloud Computing*) e a Computação na Neblina (*Fog Computing*) (MOHAN; KANGASHARJU, 2017)

Antes de adentrar mais especificamente em cada camada que compõe a Internet das Coisas, assista a vídeoaula a seguir, na qual você se contextualizará sobre as formas de conexão à internet.

Videoaula: Modelos de Computação para Dispositivos na IoT

Na computação em nuvem, segundo Hassan (2018), o desempenho computacional, armazenamento, *software* e demais serviços são fornecidos em uma rede (principalmente a internet) como um grupo de recursos virtualizados. A "nuvem" de recursos pode ser acessada a qualquer momento e de qualquer local por um dispositivo conectado.

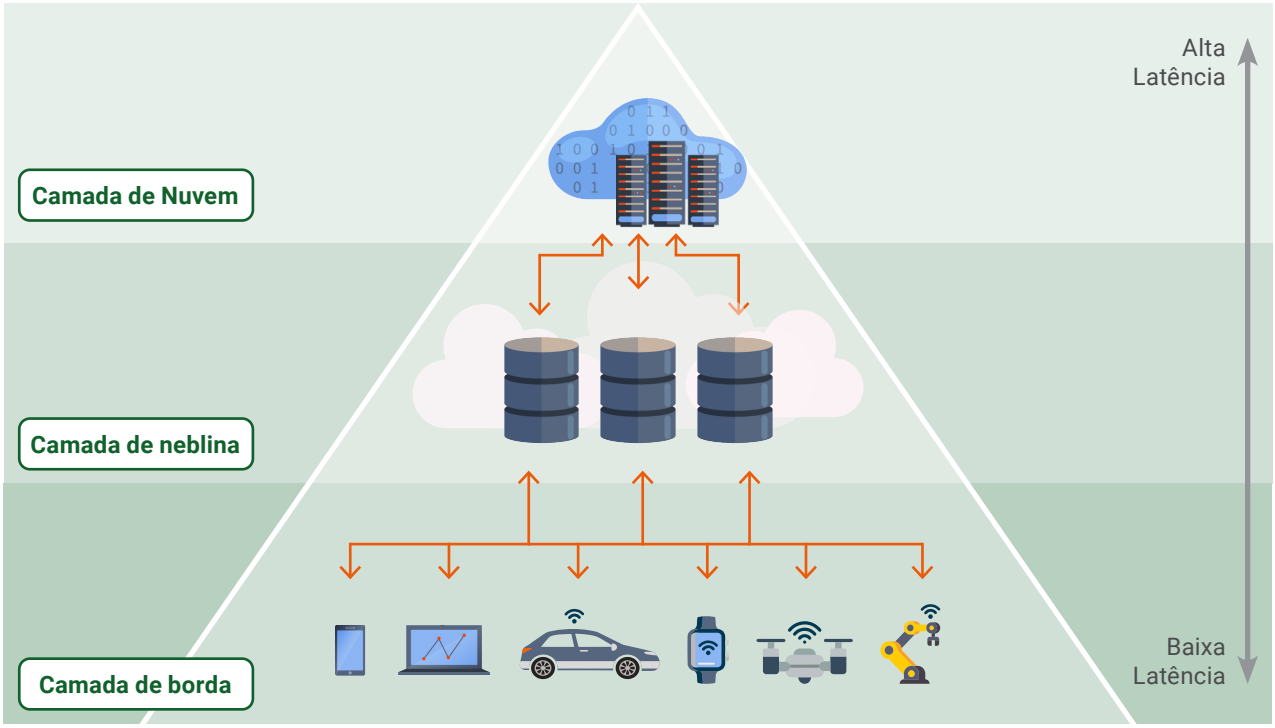
DESTAQUE

Para trazer um exemplo mais próximo do que é computação em nuvem, analise o fato de que atualmente é possível utilizar recursos que no passado necessitavam de instalação local nos computadores. Na década 90, por exemplo, para utilizar uma planilha eletrônica, como o Excel, você adquiria uma mídia com o *software*, realizava a instalação na máquina e, a partir de então, o programa estava disponível para a utilização. Hoje, é possível acessar o Pacote Office de forma *online*, pois ele está disponível na "nuvem", disponibilizado como um serviço pela Microsoft, a empresa fabricante do *software*. É possível ainda utilizar um recurso similar e gratuito, como é o caso das planilhas do Google. Os serviços citados não precisam ser acessados diretamente por um computador, mas também por meio de *tablets* ou *smartphones*. Outra realidade que mudou nas últimas décadas com o surgimento da computação em nuvem foi a forma de armazenamento e troca de arquivos. Há algum tempo, eram utilizadas mídias físicas, como disquetes, CDs e *pendrives* (dispositivos USB), você é dessa época? Atualmente essas mídias foram substituídas por contas no Google Drive, da Google, ou no One Drive, da Microsoft, por exemplo.

> Apesar de todas as vantagens e benefícios da computação em nuvem, ela é de natureza centralizada, fato que a torna ineficiente para aplicativos sensíveis à latência (atraso na resposta) em termos de transferência e processamento de dados (AL-QAMASH *et al.*, 2018).

Na busca por resolver as limitações da computação em nuvem, a empresa Cisco introduziu, em 2012, o conceito de *Fog Computing* ("computação em neblina", em português), que permite o processamento local de dados estendendo a arquitetura tradicional de computação em nuvem para a borda da rede (AL-QAMASH *et al*., 2018), reduzindo o grau de envolvimento da nuvem. Isso significa que unidades de processamento são utilizadas mais próximas dos dispositivos finais, permitindo melhorar a utilização da potência computacional, o tempo de execução de tarefas e o tempo de processamento.

A figura a seguir traz um esquema que demonstra a "posição" que a camada de computação em neblina ocupa em relação à nuvem:



Camadas *Cloud* (nuvem), *Fog* (neblina) e *Edge* (borda) de computação.
Elaboração CEPED/UFSC (2022). Adaptado de Shutterstock.com

Conforme é possível observar na figura, a ideia de neblina é justamente ser uma camada de nuvem mais distribuída e próxima à borda, em que os dispositivos conectados se encontram. Assim, pode-se dizer que há um pré-processamento na camada de neblina, que consegue reduzir a carga de processamento que seria exigida da nuvem.

É possível também ter uma noção sobre o conceito da computação de borda (*edge computing*), também referenciada como local: ela está localizada praticamente junto aos dispositivos finais que consomem os serviços e que geram e recebem os dados que serão trocados com a nuvem.

Conforme Mohan e Kangasharju (2017), a camada *Edge* (borda) é a mais externa da nuvem, sendo constituída por recursos operados por humanos, como *desktops*, *laptops*, *nano data centers, tablets* etc. Esses recursos estão localizados a uma distância de um ou dois "saltos" dos sensores e clientes IoT. Na camada de borda, assume-se que a conectividade ocorre na forma “dispositivo a dispositivo”, com uma conexão confiável com a camada de neblina.

DESTAQUE

O termo “salto” se refere a um caminho entre origem e destino. Quando você envia dados pela internet, os pacotes de dados precisam passar por vários roteadores (caminhos) antes de chegar ao destino final (um servidor, por exemplo). Cada vez que o pacote é encaminhado para o próximo roteador, ocorre um salto.

Uma comparação considerando os requisitos funcionais das computações em nuvem, em neblina e de borda foi apresentada por Al-Qamash et al. (2018), especificamente sobre o desempenho de cada tipo de computação. Os autores afirmam que:

> “- Na computação em nuvem, o congestionamento ou falhas dos servidores ao processar podem afetar o serviço da nuvem e aumentar o atraso;
>
> - A computação em neblina suporta resposta rápida, com baixa latência e baixo requerimento de largura de banda (consumo de dados);
>
> - A computação de borda suporta a resposta no mais curto tempo, com um processamento mais eficiente e com menor pressão na rede, o que garante melhor atuação.”

SAIBA MAIS

A Cisco é uma grande empresa que desenvolve equipamentos de comunicação e que foi citada nesta unidade. Para conhecer mais sobre IoT e redes, acesse o vídeo, produzido pela própria empresa clicando aqui.

Enfim, cada um dos modelos de computação apresentados possui suas características de funcionamento, implementação e apresenta suas performances individuais. Este tópico apresentando na unidade traz um caráter técnico, mas que é essencial para que você possa tomar decisões sobre uma possível implementação em uma rede IoT.

Agora, exercite sua capacidade de abstração imaginando uma possível implementação de uma rede IoT no setor em que você atua:

Implementação de uma rede IoT.

Elaboração: CEPED/UFSC (2022). Adaptado de Freepik.com

Encare essas questões como um exercício que conseguirá situá-lo(a) em relação ao conteúdo e trazer problemas reais que podem ser resolvidos com a utilização da teoria apresentada!

1.3 Coisas que podem se conectar

> O número de "coisas" que podem se conectar à internet aumenta cada vez mais. Quando a internet surgiu, somente os computadores se conectavam à rede e, por volta de 1974, as máquinas de autoatendimento (*Automated Teller Machines*, ATMs) foram os primeiros dispositivos "inteligentes" que se conectaram a uma rede, ou seja, ficaram "online" (HASSAN, 2018, p. 4).

Atualmente, pode-se listar os seguintes dispositivos:

- *Smartphones;*
- *Smartbands;*
- *Wearables;*
- Assistentes por comando de voz;
- *Smart TVs;*
- Consoles de games (por exemplo, PlayStation e Xbox);
- Aparelhos de IPTV; e uma gama infinita de outros dispositivos.

Trabalhos como o de Ejaz *et al*. (2016) já previam a conexão de alguns bilhões de dispositivos à internet em 2020, indicando que estes números devem crescer ainda mais graças ao surgimento de novas tecnologias, como as redes de comunicação 5G. Além de permitir conexões de alta velocidade, as redes 5G possibilitarão que novos serviços sejam criados, impulsionando novos produtos e novos ecossistemas tecnológicos, inclusive relacionados à IoT.

As redes 5G vão possuir baixa latência, que é o tempo gasto (geralmente medido em milissegundos (ms) para que um dispositivo conectado à rede móvel obtenha retorno da fonte de transmissão (torre de transmissão da rede celular, ou de um link de rádio, por exemplo).

A IoT está rapidamente se tornando uma realidade que conecta qualquer coisa a qualquer outra coisa – dispositivos (relógios, óculos, pulseiras), eletrodomésticos (geladeiras, televisores), sensores, carros autônomos, dispositivos móveis (drones) – a qualquer hora e em qualquer lugar, assim como destacam Parvez *et al*. (2018), que afirmam que os dispositivos estão conectados a um mundo "hiper-sempre-conectado". Embora as operadoras estejam oferecendo suporte a aplicativos IoT por meio das redes atuais, somente com a redução de latência proporcionada com as redes 5G uma expansão significativa irá ocorrer.

E você, quais dispositivos conectados à internet costuma utilizar? Somente seu *smartphone*? Possui um *smartwatch* ou uma assistente pessoal como a Alexa em sua residência? Assiste a filmes em uma *smart* TV ou utiliza um dispositivo IPTV? Sua casa é automatizada? Possui sensores de presença, acionamentos por comando de voz e câmeras de vigilância que podem ser acessados pela internet? Seus eletrodomésticos já estão conectados? Sabia que já existem geladeiras que podem avisar ao proprietário que determinado item está no fim e precisa ser comprado, ou que ele já passou do prazo de validade?

Conceito de dispositivo de comunicação.

Fonte: Freepik.com

Os comunicadores utilizados pela tripulação da nave *Enterprise*, da série *Star Trek*, eram somente ficção científica na década de 1960, mas se transformaram em realidade com o surgimento da telefonia celular. Quanto tempo ainda vai demorar para termos dispositivos como o conceito apresentado na figura apresentada anteriormente? Estamos cada vez mais conectados. Será que o *smartphone* e outros dispositivos que nos conectam à internet passaram a ser uma "extensão de nosso corpo", como previu o visionário Steve Jobs?

O que pode se conectar à internet e ser considerada uma “coisa” conectada? A resposta é: praticamente tudo! Para o consumidor, a cada dia surgem novas possibilidades de adquirir dispositivos que podem se conectar à rede. Mas, além do que é disponibilizado comercialmente, existem dispositivos eletrônicos que permitem conectar à internet praticamente qualquer coisa que você quiser.

Um dispositivo que permite criar conexões à IoT é o ESP8266, que consiste em uma pequena placa que pode ser programada e, através de pinos, pode receber e enviar sinais elétricos/eletrônicos. Com estes sinais, é possível desenvolver um sistema de automação residencial, criar um alimentador automático para um pet e permitir que ele seja acionado dentro de horários específicos, ou até mesmo acessar uma câmera que vai permitir interagir com o animalzinho enquanto ele se alimenta!

Um dispositivo como o ESP8266 pode ser utilizado por um hobbista para desenvolver uma ideia, ou até para transformar esta ideia em um produto comercial, que pode se transformar em um negócio. O mercado de desenvolvimento de dispositivos IoT, assim como de aplicativos para controle e comunicação com os dispositivos, é extremamente promissor e conta com vasto material didático.

Por exemplo, Schwartz (2016) traz uma série de projetos com o ESP8266 que podem servir como base para o desenvolvimento de aplicações residenciais e comerciais relacionadas à IoT. Dentre as propostas do autor, encontram-se um sistema de armazenamento de dados em nuvem, um controle de pontos de iluminação via internet e uma tranca de porta acionada por um servidor armazenado em nuvem.

DESTAQUE

Vamos explorar um pouco mais este conceito de que “qualquer coisa pode se conectar” e extrapolar a ideia para um setor governamental como o da saúde pública? Imagine poder fazer o monitoramento online de pacientes com doenças crônicas e conseguir priorizar atendimentos, entregas de medicação e ordens de atendimentos hospitalares e consultas? Um paciente com diabetes, por exemplo, poderia ter um sensor IoT conectado à rede, transferindo as informações em tempo real para um centro de monitoramento e, dependendo dos índices de glicose no sangue, o médico indicaria alterações no tratamento ou verificaria a necessidade de algum atendimento de urgência. Seria uma grande evolução nos serviços de saúde, que garantiriam maior qualidade à população, bem como dinamismo e economia ao setor governamental.

Ressalta-se novamente, a verdadeira transformação digital passa por uma reformulação na mentalidade da organização, com a adoção da IoT no setor de saúde do governo sendo um exemplo perfeito. Para o sucesso desta empreitada seria necessário iniciar pela colocação da tecnologia como pilar central do setor de saúde, considerando todos os ganhos que estatraria ao setor.

Com um planejamento solido e investimentos adequados seria necessário a condução de estudos de caso e de projetos piloto que permitissem medir a eficiência trazida pela transformação digital no setor. Posteriormente um ciclo PDCA poderia ser conduzido para aprimorar as ações.

SAIBA MAIS

Acesse os materiais sugeridos aqui. O primeiro é sobre sensores IoT utilizados para facilitar a vida de pacientes que já são uma realidade, como é o caso do sistema Freestyle Libre da empresa Abbott, que reduz a necessidade de furações com lancetas para os pacientes com diabetes (veja aqui).

Assim como a proposta anterior, que sugeriu imaginar possíveis aplicações no setor público de saúde, você pode estender esta análise para diversos outros setores, como transportes, segurança, mobilidade urbana. A partir disso, é possível concluir que realmente "quase tudo pode se conectar". Um panorama sobre aplicações IoT e de dispositivos que podem se conectar são apresentados no vídeo, do canal Olhar Digital disponível aqui.

Você chegou ao final desta unidade. Nela, você aprendeu como os dispositivos IoT se conectam em rede, quais os modelos de computação disponíveis para as redes e quais são os dispositivos que podem se conectar a uma rede IoT. Continue firme nos estudos!

Referências

ABOUSALEM, Z. Z.; ASHABRAWY, M. A.. Compared Between Ipv6 And With Ipv4,Differences And Similarities. **International Journal Of Computers & Technology**, [S.l.], v. 2, n. 17, p. 7340-7348, 2018. Disponível em: https://www.researchgate.net/publication/328707868_Compared_Between_Ipv6_And_With_Ipv4Differences_And_Similarities. Acesso em: 24 jan. 2022.

AL-QAMASH, Amal; SOLIMAN, Iten; ABULIBDEH, Rawan; MOUTAZ, Saleh. Cloud, Fog, and Edge Computing: A Software Engineering Perspective. Beirut: **2018 International Conference on Computer and Applications (ICCA)**, 26 jul. 2018. Disponível em: https://www.researchgate.net/publication/327638413_Cloud_Fog_and_Edge_Computing_A_Software_Engineering_Perspective. Acesso em: 24 jan. 2022.

BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL (BNDES). **Produto 8: Relatório do Plano de Ação** – Iniciativas e projetos mobilizadores. Rio de Janeiro, 2017. Versão 1.1. 65 p. Disponível em: https://www.bndes.gov.br/wps/wcm/connect/site/269bc780-8cdb-4b9b-a297-53955103d4c5/relatorio-final-plano-de-acao-produto-8-alterado.pdf?MOD=AJPERES&CVID=m0jDUok. Acesso em: 21 jan. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 jan. 2022.

BRITO, Lucas L. Freire; NETO, Milton M.; OLIVEIRA, Monica Rocha F.; MORAES, Igor A.; MUNIZ, Vinicius Angelo de O. Protocolos de Comunicação para Internet of Things (IoT). **Intercursos Revista Científica**, [S. l.], v. 17, n. 1, 2019. Disponível em: https://revista.uemg.br/index.php/intercursosrevistacientifica/article/view/3712.
Acesso em: 24 jan. 2022.

Cisco IoT Networking Overview. [S.l.]: Cisco IoT, 2019. (2 min.), son., color. Disponível em: https://www.youtube.com/watch?v=XYD-rHkCfyM. Acesso em: 24 jan. 2022.

EJAZ, Waleed; ANPALAGAN, Alagan; IMRAN, Muhammad Ali; JO, Minho. Internet of Things (IoT) in 5G Wireless Communications. **IEEE Access**, [S.l.], v. 4, p. 10310-10314, 2016. Disponível em: https://www.researchgate.net/publication/313112342_Internet_of_Things_IoT_in_5G_Wireless_Communications. Acesso em: 24 jan. 2022.

HASSAN, Qusay F. **Internet of Things A to Z**: Technologies and Applications. New Jersey: John Wiley and Sons, 2018.

Internet das coisas: no futuro, tudo será conectado. Olhar Digital, 2020. (7 min.), son., color. Disponível em: https://www.youtube.com/watch?v=hJwZpq-6jmI. Acesso em: 24 jan. 2022.

MODELO OSI e TCP/IP - Como funciona o processo de comunicação em redes. Redes Brasil, 2016. (20 min.), son., color. Disponível em: https://www.youtube.com/watch?v=oz8gvGIUKFw. Acesso em: 24 jan. 2022.

MOHAN, Nitinder; KANGASHARJU, Jussi. Edge-Fog Cloud: A distributed cloud for Internet of Things computations. Paris: **2016 Cloudification of Internet of Things**, 2016. Disponível em: https://www.researchgate.net/publication/313879300_Edge-Fog_Cloud_A_Distributed_Cloud_for_Internet_of_Things_Computations. Acesso em: 24 jan. 2022.

PARVEZ, Imitiaz; RAHMATI, Ali; GUVENC, Ismail; SARWAT, Arif I.; DAI, Huayiu. A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions. **IEEE Communications Surveys & Tutorials**, v. 20, n.4, p. 3098-3130, 2018. Disponível em https://ieeexplore.ieee.org/document/8367785. Acesso em 24 jan. 2022.

SALAZAR, Jordi; SILVESTRE, Santiago. Internet of Things. **TechPedia**. Prague: Czech Technical University of Prague, Faculty of Electrical Engineering, 2017. 31 p. Disponível em: http://techpedia.fel.cvut.cz/single/?objectId=120. Acesso em: 21 jan. 2022.

SCHWARTZ, Marco. **Internet of Things with ESP8266**. Build amazing Internet of Things projects using the ESP8266 Wi-Fi chip. Birmingham/Mumbai: Packt Publishing, 2016.

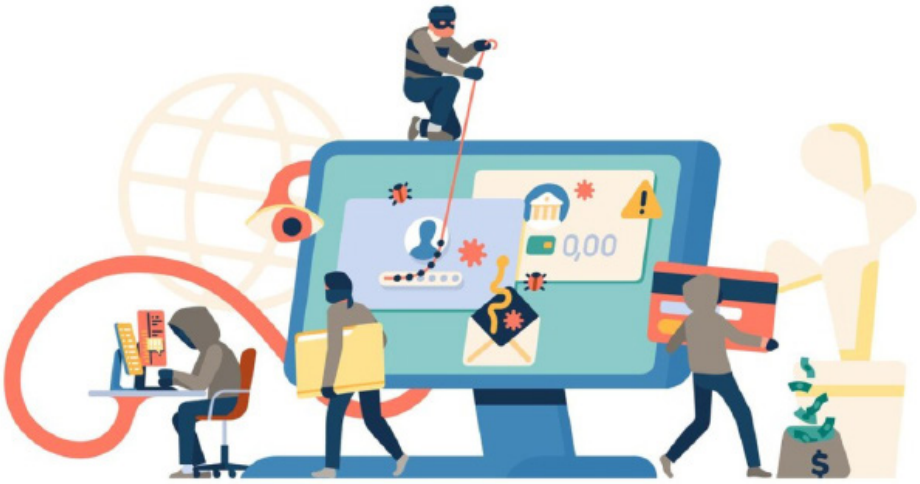
Unidade 2: Segurança e Privacidade

Objetivo de aprendizagem

Ao concluir esta unidade você estará apto(a) a reconhecer a importância da segurança e privacidade no contexto da IoT. Vamos começar?

2.1 Segurança e Privacidade no uso da IoT

A IoT "herdou" da internet todas as boas características, como a capacidade de conectar dispositivos e transferir informações (dados) entre eles. Mas outras características não tão boas foram herdadas também, como problemas de segurança: infecção por vírus, furto de informações pessoais e vazamento de dados privados.



Herança da internet
Fonte: Freepik.com

Uma vez que a IoT compartilha das mesmas questões de segurança que a internet "normal", é compreensível que os protocolos de comunicação e gerenciamento adotados em redes IoT já forneçam uma série de serviços básicos de segurança (HASSAN, 2018). Salazar e Silvestre (2017, p. 15) destacam que o surgimento da IoT

foi um marco importante e que exige novas abordagens regulatórias para garantir a privacidade e segurança dos dados de usuários.

Você já passou por alguma situação em que um problema de segurança lhe causou prejuízo, como a clonagem de um cartão de crédito ou de um conta de rede social, como Facebook ou WhatsApp? Um golpe bastante comum atualmente é o "sequestro" da conta de WhatsApp por *hackers*. Uma vez que temos diversos contatos em nossas redes sociais e muitas vezes elas são utilizadas também para atividades profissionais, ter uma conta sequestrada é uma situação extremamente desagradável.

> **Atualmente, as empresas reúnem e utilizam cada vez mais dados de clientes, o que gera riscos de segurança adicionais. As chamadas "ciberameaças", que costumavam ser tratadas apenas como um problema da área de tecnologia da informação (TI), agora são um problema da alta gestão das empresas (ROGERS, 2017, p. 147).**

Como um exemplo do porquê as empresas se preocupam cada vez mais com a segurança dos dados de seus clientes, Rogers (2017, p. 147) cita a violação de dados com roubo de informação de 40 milhões de cartões de crédito de clientes ocorrido em 2013 na empresa Target (rede de lojas dos Estados Unidos).

O problema, inicialmente da área de TI, resultou em uma grande perda de reputação da empresa, com os consumidores se afastando da marca no auge das compras de Natal e Ano Novo, forçando o CEO a renunciar.

Os problemas citados anteriormente são mais comuns na utilização de computadores e *smartphones*, mas algumas variações também podem acontecer em conexões de dispositivos IoT, e problemas com dispositivos IoT podem ser tão graves quanto os que ocorrem nas conexões usuais com a internet.

Suponha que você possui um monitoramento por câmeras em sua residência e que as elas são acessadas por IP. Essas câmeras poderiam ser *hackeadas* e as imagens de monitoramento de sua residência seriam acessadas por alguém, expondo sua privacidade e sua rotina diária.

Esses problemas de segurança, por mais que sejam incômodos para aqueles que os vivenciaram, são de "pequenas proporções" comparados a um ataque realizado ao sistema de uma usina nuclear, por exemplo!

SAIBA MAIS

Veja aqui um breve resumo do incidente de segurança relatado por Zetter (2017) sobre uma "arma digital" chamada Stuxnet. O Stuxnet era um tipo de vírus de computador criado para atacar sistemas específicos: sistemas supervisórios (SCADA) que controlavam os Controladores Lógicos Programáveis (CLPs), os quais realizavam o acionamento de centrífugas de enriquecimento de urânio.

Os sistemas SCADA, do inglês *Supervisory Control and Data Acquisiton*, são *softwares* que permitem a criação de aplicações gráficas que controlam e se comunicam com dispositivos industriais como os CLPs. Estes, por sua vez, são dispositivos de controle que recebem uma programação e permitem ligar e desligar motores com temporizações associadas, por exemplo.

O Stuxnet não representava perigo aos computadores pessoais, pois foi projetado para atacar um sistema específico. Após ter se espalhado por milhares de computadores no mundo, a arma digital atingiu seu objetivo principal em uma instalação em Natanz, no Irã. É incrível o fato de que os CLPs, que podem ser considerados nós IoT, não estavam conectados diretamente à internet e mesmo assim foram infectados, pois o vírus foi transportado de forma específica em unidades de armazenamento USB (*pendrives*).

Como efeito do vírus, as centrífugas giravam em uma velocidade superior àquela para a qual haviam sido projetadas e, consequentemente, acabavam sendo danificadas dentro de um período inferior ao estimado. Esse evento foi considerado como um indício de que a guerra cibernética havia começado.

DESTAQUE

A partir do exemplo do ataque pelo Stuxnet e dentro do contexto da IoT, quais são os limites desta guerra? Uma empresa poderia criar um novo vírus capaz de se instalar e degradar os equipamentos de uma concorrente? Um governo poderia obter informações privilegiadas de um regime político de oposição por meio do hackeamento das redes de sensores e bancos de dados?

Mas... se a IoT foi desenvolvida a partir da "internet original", não seria possível simplesmente "copiar" as soluções de segurança e aplicá-las na conexão de dispositivos IoT? Infelizmente, a solução não é tão simples assim.

Conforme destacado por Pinto Junior, Silva e Xavier (2017), a maneira mais comum de estabelecer uma conexão IoT é através de uma rede *wireless*, que possui diversos problemas de segurança. Muitos deles possuem soluções satisfatórias, porém limitadas, como é o caso de criptografia assimétrica, que exige elevado poder computacional.

Em um folheto de soluções empresariais para IoT, a Alcatel-Lucent Enterprise (2019) indica que o crescimento dessa tecnologia intensificou a quantidade de ameaças à segurança cibernética, já que a proliferação de sensores e dispositivos conectados expande a superfície de ataque na rede.

Os sistemas de IoT representam o elo mais fraco na segurança da rede corporativa, pois muitos dos dispositivos conectados à IoT são fabricados sem ter o requisito de segurança como prioridade e, muitas vezes, são desenvolvidos por empresas que não entendem os requisitos de segurança atuais.

Serpanos e Wolf (2018) corroboram os problemas de segurança associados aos dispositivos IoT, já que esses sistemas possuem ferramentas de segurança inferiores aos dos sistemas convencionais. Os autores adicionam ainda o fato de que os "nós" de uma rede IoT, assim como os sensores, possuem uma vida útil de vários anos e, consequentemente, vão estar suscetíveis a problemas de segurança durante bastante tempo.

> **Uma das causas para os problemas de segurança associados aos dispositivos IoT, como sensores, cartões inteligentes e outros, é o seu baixo poder computacional, que não os permite processar os algoritmos de criptografia convencionais, exigindo novas propostas de segurança, assim como as soluções do tipo "leves" (*lightweight*) (PINTO JUNIOR, SILVA; XAVIER, 2017).**

Essas soluções "leves", segundo Pinto Junior, Silva e Xavier (2017), são caracterizadas por técnicas, arquiteturas e tecnologias que são leves em termos de exigência de processamento dos dispositivos que as processam, habilitando assim itens com baixo poder de processamento para utilizar estas soluções. A

preocupação de como a proteção para os dispositivos conectados à IoT será implementada extrapola a esfera técnica e passa a ser compartilhada entre fabricantes de equipamentos, usuários e governos.

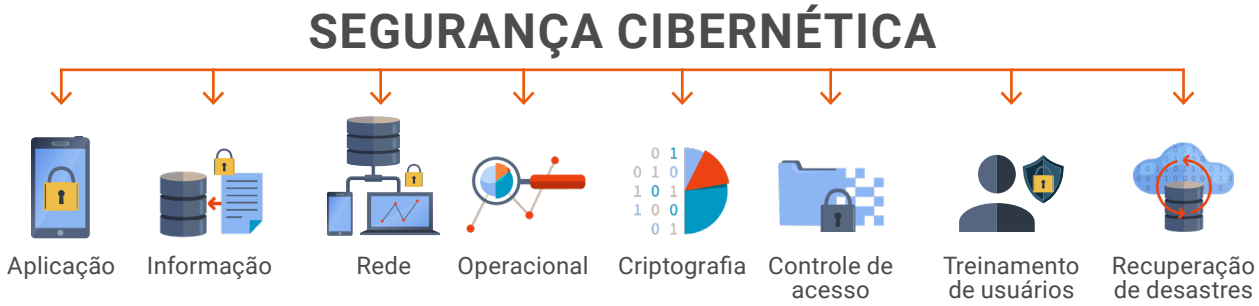
Como exemplo de uma preocupação a nível governamental, Holdowsky *et al*. (2015, p. 16) citam que:

> **entidades que coletam e armazenam dados são responsáveis e devem implantar sistemas de segurança para evitar qualquer acesso não autorizado, modificação, exclusão ou uso dos mesmos. Porém, com relação ao ecossistema de IoT, não está claro quem irá projetar, desenvolver e implementar os padrões regulatórios necessários.**

Os autores falam que já se discute a adaptação de diretrizes de segurança existentes, verificando se estas são adequadas para aplicativos de IoT em evolução. Mas, no caso da Lei de Portabilidade e Responsabilidade do Seguro Saúde nos Estados Unidos, que rege a proteção de informações médicas coletadas por médicos, hospitais e seguradoras, não há consenso sobre estender a regência da lei às informações coletadas por meio de *wearables*, por exemplo.

> **A segurança e a privacidade dos dados terão um papel importante nas implantações de sistemas IoT, os quais irão produzir e lidar com informações de identificação pessoal, segurança de dados e privacidade, assim como previsto por Minerva, Biru e Rotondi (2015, p. 6).**

Os serviços e aplicativos, segundo Minerva, Biru e Rotondi (2015), serão desenvolvidos com base na poderosa plataforma da IoT, exigindo segurança para o atendimento dos negócios que irão ser gerados com esta tecnologia. De forma geral, a IoT pode ter um impacto na sociedade, exigindo restrições e regulamentações que devem ser formuladas para cada país.



Representação de itens relacionados à segurança em uma rede.
Elaboração: CEPED/UFSC (2022)

Para avaliar a importância da regulamentação da segurança envolvida em uma rede IoT, vamos analisar a questão da Lei Geral de Proteção de Dados (LGPD), que está em vigor no Brasil desde 2019, incluída pela Lei nº 13.853. A legislação traz, em seu texto, um caráter fundamental que se refere à proteção de dados pessoais.

Desde a sanção da lei, as empresas devem deixar claro ao consumidor como os dados estão sendo coletados e como serão utilizados, entre outras informações. Com este tipo de procedimento, deve-se – teoricamente – evitar que os dados pessoais dos consumidores sejam utilizados de forma indevida por empresas e/ou acabem sendo acessados por serviços e/ou pessoas que possam utilizá-los de forma prejudicial à privacidade.

Nesse contexto, é fundamental observar que, por ser uma Lei Federal, a LGPD garante a regulamentação de serviços e atividade que envolvam dados pessoais, amenizando atividades criminosas à privacidade do cidadão.

SAIBA MAIS

Para se aprofundar na discussão sobre a LGPD e sua aplicação em diferentes esferas, veja a gravação do webnário sobre Aplicação da Lei Geral de Proteção de Dados Pessoais no Judiciário, realizado pelo Superior Tribunal de Justiça (STJ), disponível aqui.

DESTAQUE

Assim como a LGPD, outras leis que regulamentem os serviços e o ecossistema das redes IoT serão necessárias futuramente, garantindo que, ao criar um produto/serviço que utilize dados que trafegam em uma rede IoT, as informações e dados pessoais estejam seguros. Talvez uma primeira alternativa para criar uma regulamentação de serviços IoT possa ser derivada da própria LGPD, a qual possui, em termos genéricos, itens sobre a proteção de dados que são similares a alguns serviços que podem ser oferecidos via redes IoT. Como proposta de reflexão sobre o assunto, destaque comparações da LGPD com as necessidades de segurança no ecossistema IoT.

A preocupação com os dados percorre uma longa cadeia de interesses que envolvem usuários, empresas que fornecem equipamentos, empresas que oferecem serviços e gestores públicos que precisam garantir a regulamentação destes serviços. Com a regulamentação, haverá o incentivo ao crescimento do ecossistema IoT de forma segura e benéfica à sociedade, aos negócios, indústrias e, consequentemente, ao próprio poder público.

As informações pessoais, transações bancárias e dados profissionais trafegam por redes que precisam oferecer proteção contra ataques de *hackers*, vírus e outras ameaças digitais. Da mesma forma, as redes IoT precisam de proteção equivalente para poderem se desenvolver e oferecer serviços confiáveis aos seus usuários.

Você chegou ao fim desta unidade, na qual aprendeu a respeito da importância da segurança e privacidade no contexto da IoT. Em um mundo cada vez mais conectado, a segurança em operar com dados pessoais é fundamental. Agora, faça uma verificação de como foi sua aprendizagem. Execute as atividades disponibilizadas no ambiente virtual e veja se você compreendeu os principais pontos desenvolvidos.

Referências

A Aplicação da Lei Geral de Proteção de Dados Pessoais no Cotidiano do Poder Judiciário e do STJ. Superior Tribunal de Justiça (STJ). 2020. (80 min.), son., color. Webinário. Disponível em: https://www.youtube.com/watch?v=uhLLtb2AINM. Acesso em: 25 jan. 2022.

ALCATEL-LUCENT ENTERPRISE (ALE). **A Internet das Coisas (IoT) nas Empresas**: Crie uma base segura para aproveitar as oportunidades de negócios da IoT. 2019. Resumo da Solução IoT para Empresas. Disponível em: https://www.al-enterprise.com/-/media/assets/internet/documents/iot-for-enterprise-solutionbrief-ptbr.pdf. Acesso em: 25 jan. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 jan. 2022.

HASSAN, Qusay F. **Internet of Things A to Z**: Technologies and Applications. New Jersey: John Wiley and Sons, 2018.

HOLDOWSKY, Jonathan; MAHTO, Monika; RAYNOR, Michael J.; COTTELEER, Mark. **Inside the Internet of Things (IoT)**: A primer on the technologies building the IoT. Westlake: Deloitte University Press, 2015.

MINERVA, Roberto; BIRU, Abyi; ROTONDI, Domenico. **Towards a definition of the Internet of Things (IoT)**: Revision 1 - Published 27 May 2015. IEEE Internet Iniciative, 2015. 86 p. Disponível em: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf. Acesso em: 21 jan. 2022.

PINTO JUNIOR, Joelias S.; SILVA, Clerisson dos Santos e; XAVIER, Danilo Domingos. Segurança em Internet das Coisas: Um survey de soluções lightweight. **Revista de Sistemas e Computação – RSC**. Salvador, v. 7, n. 2, p. 365-384, 2017. Disponível em https://revistas.unifacs.br/index.php/rsc/article/view/5110. Acesso em: 25 jan. 2022.

ROGERS, David L. **Transformação digital: repensando o seu negócio para a era digital**. 1ª ed. São Paulo: Autêntica Business, 2017.

SALAZAR, Jordi; SILVESTRE, Santiago. Internet of Things. **TechPedia**. Prague: Czech Technical University of Prague, Faculty of Electrical Engineering, 2017. 31 p. Disponível em: http://techpedia.fel.cvut.cz/single/?objectId=120. Acesso em: 21 jan. 2022.

SERPANOS, Dimitrios; WOLF, Marilyn. **Internet-Of-Things (Iot) Systems**: Architectures, Algorithms, Methodologies. 1st ed. New York: Springer, 2018.

ZETTER, Kim. **Contagem Regressiva até Zero Day**: Stuxnet e o lançamento da primeira arma digital do mundo. 1ª ed. Rio de Janeiro: Brasport, 2017.