



Módulo de Aprendizagem [Internet das Coisas]

Projeto: B-SAFE

Número: 2018-1CZ01-KA204-048148

Nome do autor: EDIT VALUE®

Última data de processamento: 28.10.2020

Funded by the
Erasmus+ Programme
of the European Union



"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."



Internet das Coisas

Introdução

Abrangida pela quarta revolução industrial, a Indústria 4.0, e com um impacto mais direto para o indivíduo como utilizador final, vamos conhecer com maior detalhe o conceito da Internet das Coisas, vulgarmente conhecida como IoT (*Internet das Coisas*, em inglês).



A Internet das Coisas é um sistema de dispositivos informáticos, máquinas mecânicas e digitais, objetos, animais ou pessoas inter-relacionados que têm a capacidade de transferir dados através de uma rede sem necessidade de interação de humano para humano ou de humano para computador. O primeiro dispositivo "oficial" IoT foi uma máquina de Coca-Cola no campus da Universidade Carnegie Mellon em Pittsburgh, Pensilvânia, em 1982. Os estudantes queriam poder saber antecipadamente se as latas de refrigerantes recém carregadas estavam no pico da sua refrigeração por isso manipularam a máquina para reportar esta informação a um computador num escritório próximo.

Apesar da idade, a tecnologia IoT está em constante evolução, pelo que enfrentamos mudanças perturbadoras relacionadas com os nossos hábitos de vida, pois existe uma quantidade significativa de oportunidades e possíveis aplicações da IoT quer em ambientes industriais quer na vida quotidiana.

Embora forneça soluções eficazes e eficientes para variados problemas do mundo real, existem também desafios significativos em matéria de segurança e privacidade que não devem ser ignorados.

Relevância Prática – Assim poderás aplicar os conhecimentos e competências aqui adquiridos

Com as aprendizagens concretizadas neste módulo será possível descrever o conceito de Internet das Coisas e quais as principais aplicações desta nova tecnologia.

Além disso, serão debatidas as questões mais comuns relacionadas com a segurança e privacidade da Internet das Coisas, bem como possíveis reações no caso de um ciberataque a um dispositivo inteligente.



1.Desenvolver conhecimento – Internet das Coisas no quotidiano

Ao longo dos anos tem havido um rápido crescimento no domínio da Internet das Coisas (IoT) em termos de tecnologia, bem como no crescimento do mercado. A rede de computadores, mais conhecida como "Internet", revolucionou a forma como partilhamos a informação. A Internet das Coisas pode ser considerada a próxima revolução na forma como percebemos e partilhamos a informação (Virat, 2018). Na caixa abaixo apresenta-se uma definição simplificada de IoT:

Definição

Internet das Coisas é o conceito de ligar qualquer dispositivo (desde que tenha um interruptor *on/off*) à Internet e a outros dispositivos conectados. A Internet das Coisas é **uma rede gigante de dispositivos e pessoas ligadas - que recolhem e partilham dados** sobre a forma como são utilizadas e sobre o ambiente que as rodeia.

Dispositivos e objetos com sensores incorporados estão ligados a uma plataforma IoT, que integra dados de diferentes dispositivos e permitem partilhar as informações mais valiosas, com aplicações construídas para responder a necessidades específicas. Nas figuras abaixo encontram-se dois bons exemplos de uma tecnologia IoT.



Como vimos anteriormente, a IoT é um termo amplamente utilizado para descrever a vasta rede de dispositivos ligados à Internet que existe actualmente.

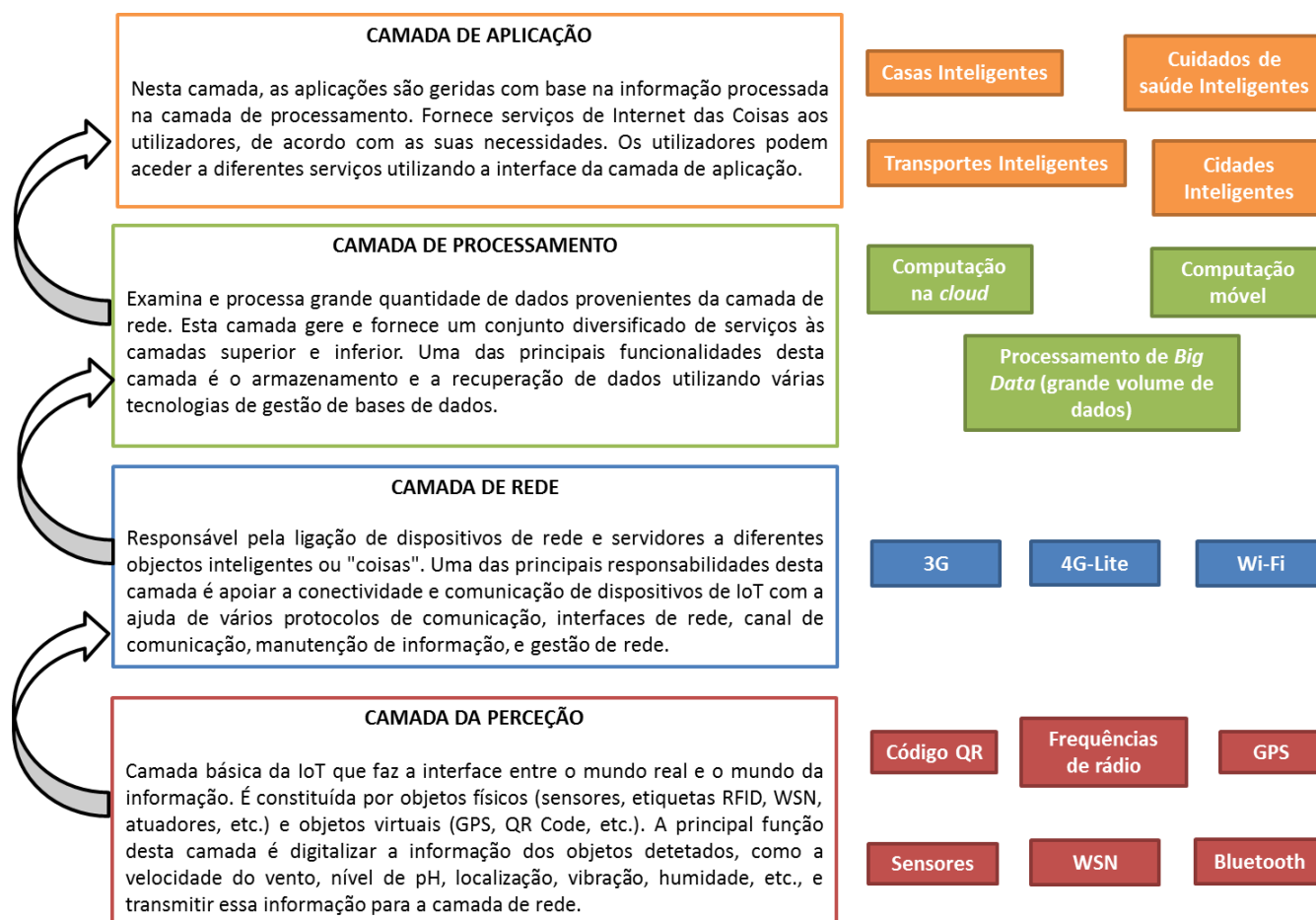


A IoT promete ser o desenvolvimento tecnológico mais importante para os consumidores desde o lançamento/aparecimento do *smartphone*. Os especialistas acreditam que esta tecnologia acabará por gerar mais de 123 mil milhões de dólares em receitas anuais até 2021 e as estatísticas apontam que haverá mais de 36 mil milhões de dispositivos ligados à Internet até ao final de 2020.

De facto, grandes empresas como a Amazon, a Google e a Tesla já estão a trabalhar com serviços de desenvolvimento de *software* para produzir dispositivos IoT de última geração. Espera-se que a IoT torne as casas inteligentes avançadas numa realidade. Mais exemplos de tecnologias IoT incluem **carros autónomos, dispositivos para usar no corpo que rastreiam marcadores corporais, a adesão de pacientes a mudanças de comportamento, assistentes de voz (a Alexa, por exemplo), sistemas de aquecimento inteligentes, etc.**

Por causa disso, podemos facilmente prever que a sociedade em geral estará em contacto com um dispositivo IoT num determinado momento. Por conseguinte, é muito **importante melhorar o comportamento global** dos cidadãos e a sua privacidade/segurança.

A dinâmica, inteligência e mobilidade da IoT tornam-na uma tecnologia com grande demanda, mas também a tornam **vulnerável e arriscada em termos de segurança e privacidade**. Para compreender a complexidade deste desafio, é necessário compreender a arquitetura básica da IoT, que se caracteriza por uma **estrutura dinâmica**. O número de camadas que compõem a arquitetura da IoT diverge imensamente entre especialistas, mas todos eles concordam que a IoT é composta por pelo menos quatro camadas: **Percepção, Rede, Processamento e Aplicação**.





Como se pode observar, a camada de aplicação facilita a gestão global das aplicações inteligentes e fornece serviços específicos ao utilizador. Na tabela seguinte são apresentadas as principais aplicações da IoT no dia-a-dia:

Casa Inteligente (<i>Smart Home</i>)	É uma casa interligada onde todos os tipos de coisas interagem umas com as outras através da Internet. Por exemplo, numa casa inteligente pode-se ligar o ar condicionado a caminho de casa ou ativar a máquina de lavar roupa à distância. No fundo, está tudo interligado para tornar a vida mais simples e conveniente.
Dispositivos usáveis (<i>Wearables</i>)	Estes dispositivos (como, por exemplo, o <i>Fit Bit</i>) recolhem dados e informações sobre o utilizador que são posteriormente pré-processados para extrair informações essenciais. Pequenos e altamente eficientes, estes cobrem amplamente os requisitos de <i>fitness</i> , saúde e entretenimento.
Carros inteligentes/conectados (<i>Smart/Connected Cars</i>)	Um veículo inteligente que é capaz de otimizar o seu próprio funcionamento, manutenção e conforto dos passageiros. Estes veículos estão a ser utilizados no transporte inteligente - que inclui vias navegáveis, ferroviárias, rodoviárias, etc. - recebendo informações em tempo real sobre estradas, acidentes, desvios e encerramentos de estradas, de forma a proporcionar a máxima segurança ao condutor e aos passageiros.
Cidades Inteligentes (<i>Smart Cities</i>)	Envolve tudo o que compõe uma cidade, como vigilância, transporte, sistemas de gestão de energia, distribuição de água, segurança urbana e monitorização ambiental. Por exemplo, o governo pode ser automaticamente informado sobre os níveis de poluição medidos ou a escassez de fornecimento de energia, etc.
Agricultura Inteligente (<i>Smart Agriculture</i>)	Os agricultores estão a utilizar os conhecimentos significativos dos dados para obter um melhor retorno sobre investimento. A deteção da humidade do solo e nutrientes, o controlo da utilização de água para o crescimento das plantas e a determinação de fertilizantes personalizados são alguns usos simples da IoT.
Gestão da energia	As redes elétricas do futuro serão não só inteligentes mas também altamente fiáveis. Nas redes elétricas inteligentes, a utilização de contadores inteligentes, portas de entrada, fichas inteligentes e aparelhos conectados ajuda a conservar recursos e a poupar dinheiro a consumidores, fabricantes e fornecedores de serviços públicos.
Cuidados de saúde inteligentes (<i>Smart Healthcare</i>)	Um sistema de saúde conectado e dispositivos médicos inteligentes são sinónimos de uma revolução para a sociedade, uma vez que tem um impacto significativo não só para as empresas, mas também para o bem-estar das pessoas em geral. A



aplicação da IoT no domínio da saúde inclui a obtenção de informações sobre parâmetros de saúde de um indivíduo, como a pressão arterial, temperatura corporal, medições de batimentos cardíacos, etc, através de dispositivos com consumo de energia ultra reduzido, altamente eficientes em termos energéticos e de pequena dimensão. Esta informação recolhida pode ser partilhada com os respetivos indivíduos e centros de saúde, para posterior ação por parte dos médicos.

1. Aplicar conhecimento

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_ Internet das Coisas no quotidiano_O1_O1:

Situação: *O que é a “Internet das Coisas”?*

Tarefa: Escolher a opção correta usando o princípio da escolha única: apenas uma resposta é verdadeira.

- A IoT é uma rede de servidores conectados que podem ser acedidos através da Internet.
- A IoT é a digitalização e automatização de cada parte de uma empresa, bem como do processo de fabrico.
- A IoT é uma rede global que liga sistemas informáticos em todo o mundo.
- A IoT é uma tecnologia incipiente que se concentra na interligação entre coisas ou dispositivos uns aos outros e aos seres humanos ou utilizadores para atingir alguns objectivos comuns.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_ Internet das Coisas no quotidiano_O1_O2:

Situação: *Quais são as principais aplicações da Internet das Coisas?*

Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Monitorização da linha eléctrica e transição inteligente de energia da rede.
- Gestão da cadeia de fornecimento de produção no retalho.
- Gestão da cadeia de abastecimento da produção na indústria transformadora.
- Regulação da água na agricultura.

2. Desenvolver conhecimento – Internet das Coisas e questões de segurança e privacidade

Os dispositivos inteligentes de consumo ligados à Internet das Coisas estão constantemente a recolher informações pessoais dos consumidores. Portanto, uma das maiores preocupações relacionadas com a implementação da Internet das Coisas na nossa vida diária está ligada à segurança e privacidade de informações pessoais e sensíveis, uma vez que o roubo de informações pessoais pode causar sérios danos a indivíduos, empresas e à sociedade em geral. A IoT é uma tecnologia ubíqua com uma arquitetura e estrutura complexas. Consequentemente, cria **novos problemas de segurança e**



privacidade, até à data considerados inofensivos ou indefinidos. Estas preocupações estão principalmente relacionadas com:

1. **As tecnologias da IoT têm uma vida útil mais longa** em comparação com os *smartphones* e os computadores.
2. Existem **vários fabricantes**, a maioria sem conhecimentos básicos ligados às Tecnologias de Informação (TI), o que resulta em problemas de interoperabilidade e de falta de higiene de segurança.
3. **Esta falta de especialização em TI** estende-se aos utilizadores finais (que são todos, na verdade, administradores de sistemas).
4. O número de dispositivos e a conectividade global exacerbam todas as questões. Na verdade, estima-se que existam 50 mil milhões de dispositivos conectados neste momento.

A segurança dos dados e a privacidade do utilizador são conceitos diferentes, mas não se excluem mutuamente. De facto, um ataque de segurança ou ciberataque compromete automaticamente a privacidade do utilizador.

Os desafios que devem ser superados para resolver as questões de segurança e a privacidade da IoT são inúmeros. Isto deve-se principalmente às muitas restrições associadas ao fornecimento de segurança e privacidade nos sistemas da IoT. No entanto, na caixa abaixo é apresentada uma breve definição desses conceitos, aplicados à IoT.

O tipo de ameaças e ataques de segurança e privacidade a que a IoT está sujeita depende das suas camadas, uma vez que cada camada tem diferentes particularidades e tecnologias associadas. No quadro seguinte é apresentado um resumo dos ciberataques mais comuns à estrutura da IoT, bem como o grau de impacto nas quatro camadas que compõem a arquitetura da IoT:

	Breve descrição	CAMADA DE PERCEÇÃO	CAMADA DE REDE	CAMADA DE PROCESSAMENTO	CAMADA DE APLICAÇÃO
Código malicioso	Qualquer código em qualquer parte de um sistema de <i>software</i> ou <i>script</i> que se destine a causar efeitos indesejáveis, violações de segurança ou danos a um sistema	Alto	Alto	Baixo	Alto
Ataque DoS	Ciberataque em que o atacante procura limitar o acesso a uma máquina ou recurso de rede	Baixo	Alto	Alto	Baixo
Informação de routers	Protocolos onde os routers podem usar para trocar informação sobre topologia de rede	Baixo	Alto	Alto	Baixo
Espionagem	Ato de escutar secretamente conversas e/ou comunicações privadas de terceiros sem o seu consentimento	Alto	Médio	Alto	Médio
Roubo de identidade	Utilização intencional da identidade de outra pessoa geralmente como forma de obter uma vantagem financeira ou outra informação pessoal	Alto	Médio	Alto	Médio
Ataque <i>Sinkhole</i>	Ameaça a segurança das RSSFs (Redes de sensores sem fios) em quase todas as	Médio	Alto	Baixo	Baixo



	camadas nos diferentes protocolos				
Ataque de <i>phishing</i>	Tentativa fraudulenta de obter informação ou dados sensíveis, normalmente através de falsificação de <i>emails</i> ou mensagens instantâneas	Baixo	Baixo	Médio	Alto

Como se pode observar, há uma grande **variedade de possíveis ataques** que podem comprometer a **segurança e a privacidade dos dispositivos IoT** com um nível de impacto diferente, dependendo da **camada**. Assim, existem desafios consideráveis que devem ser enfrentados por todas as partes envolvidas: **fabricante ou programador, governo e utilizador final da IoT**.



2. Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_ Internet das Coisas no quotidiano_O2_O1:

Situação: No que toca à segurança dos dispositivos IoT e seus utilizadores, qual das afirmações é verdadeira?

Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- A segurança dos dados é necessária quando os dados estão a ser gerados e armazenados.
- Os requisitos de segurança para aplicações de IoT devem ser aplicados em três camadas: camada de aplicação, camada de rede e camada de percepção.
- A probabilidade de ocorrer um ataque de *phishing* num dispositivo IoT é maior na camada de processamento.
- A arquitetura da IoT permite que entidades maliciosas explorem vulnerabilidades intrínsecas a cada uma das camadas da IoT.
- Um código malicioso pode afectar pelo menos três camadas.



Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_ Internet das Coisas no quotidiano_O1_O2:

Situação: Considerando a privacidade dos utilizadores da IoT, qual das seguintes afirmações é verdadeira?

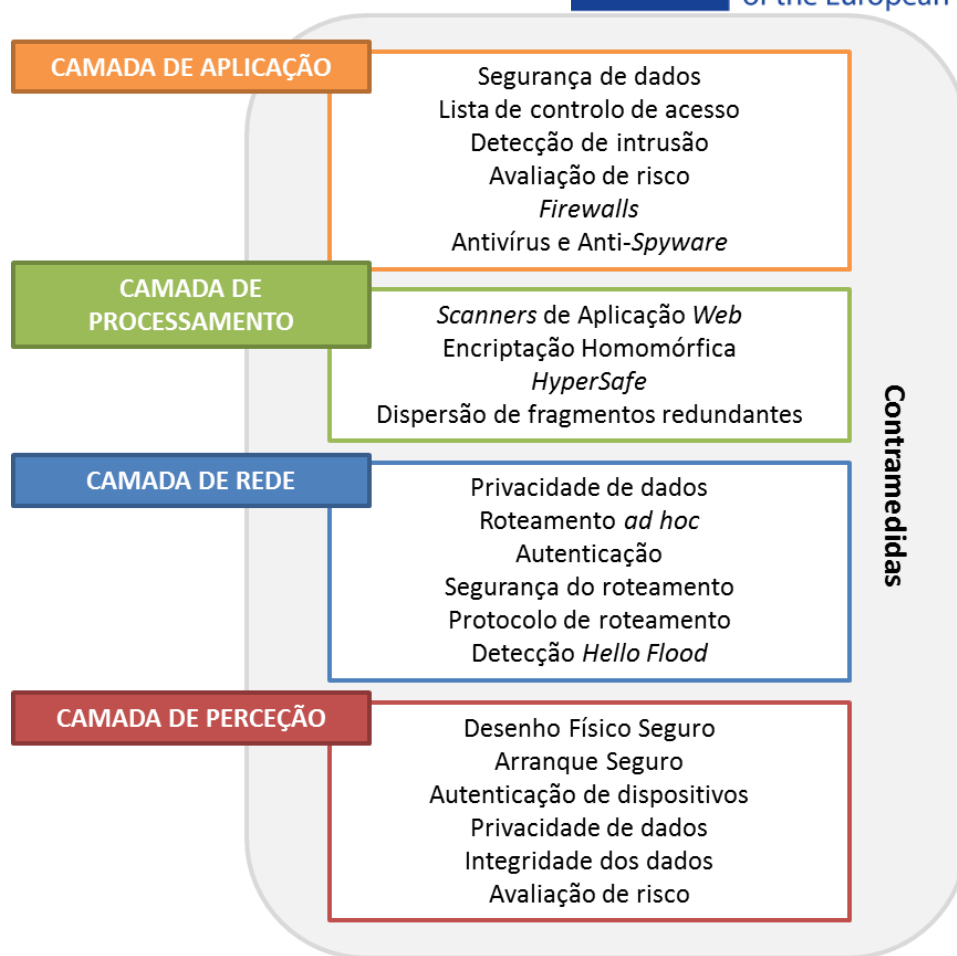
Tarefa: Escolher a opção correta usando o princípio da escolha única: apenas uma resposta é verdadeira.

- O crescimento significativo que a IoT tem mostrado durante os últimos anos trouxe várias preocupações de privacidade à medida que a disponibilidade de dados diminui, patrocinada pelas propriedades comuns e habituais da IoT.
- Os fabricantes precisam de garantir a proteção das informações pessoais associadas aos movimentos, hábitos e interações dos utilizadores.
- A privacidade refere-se à forma como os dispositivos da IoT se defendem contra o roubo de dados dos utilizadores.
- A privacidade só está em risco na camada da aplicação.

3.Desenvolver conhecimento – Internet das Coisas e a proteção dos seus utilizadores

No início do ano de 2019, a CNN conseguiu aceder a uma variedade de imagens de câmaras através de um motor de busca para dispositivos IoT, o Shodan. Observaram remotamente crianças a brincar no ginásio de uma escola básica na Indonésia, um homem a preparar-se para dormir num apartamento em Moscovo, uma família australiana e uma mulher a alimentar o seu gato no Japão. Todos eles pareciam desconhecer que as suas vidas estavam a ser transmitidas *online*, a cada segundo do dia. De acordo com a CNN, nenhuma das câmaras tinha sido submetida a verificações de segurança e estava disponível para qualquer pessoa que soubesse o endereço certo.

Para evitar que este tipo de situação lhe aconteça, existem algumas **técnicas, procedimentos e comportamentos** que deveriam ser **adotados tanto pelos programadores de dispositivos IoT como pelos usuários de dispositivos inteligentes**. Abaixo encontram-se algumas medidas para reagir e prevenir ciberataques em todas as camadas que compõem os dispositivos IoT.



Como se pode observar, a maior parte dos mecanismos de privacidade e segurança para a Internet das Coisas devem ser implementados. Os criadores da IoT devem concentrar os seus esforços na **criação de dispositivos fisicamente seguros** e protegidos com algoritmos criptográficos, plataformas de *gateway* reforçadas, encriptação complexa, antivírus, *anti-spyware*, *anti-adware* e técnicas de segurança avançadas e atualizadas. Por conseguinte, o utilizador fica dependente dos mecanismos de segurança já integrados nos dispositivos IoT para garantir a sua privacidade e segurança. No entanto, existem algumas ações que o utilizador, enquanto consumidor de dispositivos ligados à IoT, deve conhecer para ultrapassar várias ameaças à segurança e privacidade da IoT:

1º - Ler os requisitos de segurança e a política de privacidade para os dispositivos

Escolher sempre um dispositivo IoT de um fabricante transparente e de confiança. O utilizador tem o direito de conhecer as técnicas de segurança implementadas na IoT.

Além disso, deve-se sempre **ler a política de privacidade** do dispositivo, de modo a estar ciente de como funciona o dispositivo IoT e as razões pelas quais os dados pessoais estão a ser recolhidos e utilizados por dispositivos inteligentes IoT. Em termos simples, antes de utilizar um dispositivo IoT, deve-se ser capaz de saber se se pode:

- 1) Aceder, visualizar e remover os dados recolhidos através da Internet sem fios;
- 2) Desconectar os dispositivos IoT quando desejar;
- 3) Consentir no armazenamento dos dados pessoais no dispositivo IoT.

2º - Parar de usar a *password* predefinida!

A primeira coisa que se deve fazer com um dispositivo IoT é verificar se ele permite **alterar a palavra-passe predefinida**. É importante usar sempre uma senha única e forte para cada dispositivo IoT. Adicionalmente, é pertinente alterar as palavras-passe do router Wi-Fi de forma frequente.



3º - Desativar o acesso remoto (WAN) ao dispositivo

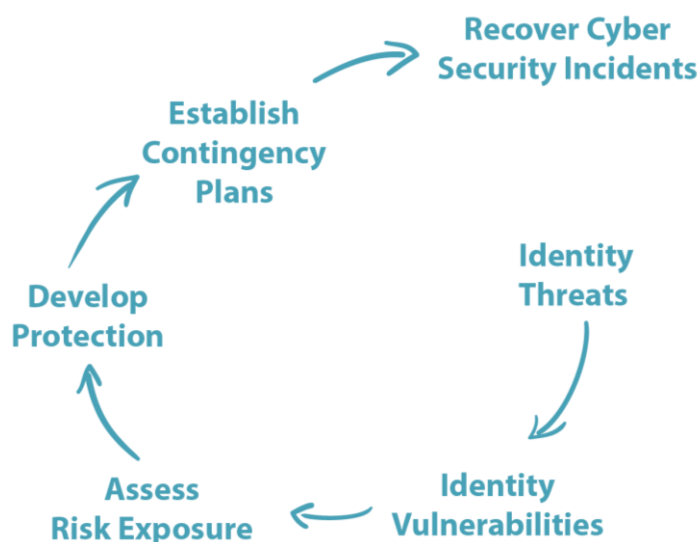
Uma pessoa que se encontre em casa e procure no Google "*qual é o meu endereço IP?*" no seu computador conseguirá ver aí o seu endereço IP WAN. Este endereço é único na Internet em qualquer altura. Se a mesma pessoa viajar para longe de casa, esse endereço IP é o que pode usar para aceder remotamente aos seus dispositivos domésticos inteligentes. Se os dispositivos não estiverem protegidos, o endereço IP é tudo o que é necessário para qualquer pessoa que queira aceder a eles. De facto, foi isso que a CNN utilizou para aceder a uma variedade de câmaras!

4º - Desativar as funcionalidades que não são usadas

Um dispositivo inteligente de confiança é um dispositivo que permite **personalizar as suas funcionalidades**. Por exemplo, se o seu relógio inteligente não estiver a ser usado para recolher os últimos dados de treino, deve-se ativar a ligação Bluetooth; ou se se estiver a registar um percurso de corrida, o GPS e a pista de localização devem ser ativados.

5º - Ser um superagente de Cibersegurança!

Sabias que 95% das violações da cibersegurança originam em erros humanos? Portanto, a **alfabetização cibernética** é a forma mais importante de eliminar os ciberataques. Um superagente de segurança cibernética deve dominar todas as fases do **plano de consciencialização cibernética**:



Quer na qualidade de utilizadores de dispositivos IoT no quotidiano, quer como proprietários ou gestores de uma empresa que usa tecnologia e Internet no seu dia-a-dia, devemos **aumentar as hipóteses de identificar um ataque à segurança ou à privacidade antes de este ser totalmente concretizado**, minimizando os danos e reduzindo os custos de recuperação.

Por esta altura, já tens todos os conhecimentos básicos para estares mais à vontade na identificação de ameaças e vulnerabilidades, na avaliação do risco e na proteção do dispositivo. Mas e se, apesar de toda a prevenção e cuidado, continuares a ser vítima de um incidente de ciberataques enquanto utilizas a IoT? A resposta depende dos **4 Q's: Quem, o Quê, Quando e Qual**.

QUEM

Faz uma lista de quem chamar no caso de um incidente. É fundamental saber quem tomará a decisão de iniciar os procedimentos de recuperação e quem será o principal contacto com os respetivos responsáveis pela aplicação da lei.



O QUÊ

Certifica-te que tens um plano para o que fazer com os teus dados no caso de um incidente. Isto pode incluir desligar e reiniciar todos os teus sistemas IoT.

QUANDO

Determina quando alertar o pessoal de emergência, profissionais de cibersegurança, prestadores de serviços ou seguradoras.

QUAL

O plano de resposta deve esclarecer quais os tipos de atividades que constituem um incidente de segurança da informação. No que respeita a uma organização, isso inclui incidentes como o facto de o *website* da mesma estar em baixo por mais do que um período de tempo especificado ou provas de um roubo de informação.

Por favor não te esqueças de envolver a família, amigos e/ou funcionários no teu plano de consciencialização cibernética, pois a **cibersegurança é da responsabilidade de cada utilizador da IoT!**

3. Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_ Internet das Coisas no quotidiano_O3_O1:

Situação: Quais as medidas de segurança que devemos implementar para evitar ciberataques nos dispositivos IoT?

Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- a) Instalar a encriptação homomórfica.
- b) Instalar *firewalls*.
- c) Criar dispersão de fragmentos redundantes.
- d) Alterar as palavras-passe pré-definidas do router.
- e) Desactivar funcionalidades no dispositivo inteligente que não estão a ser utilizadas.
- f) Desactivar o acesso remoto ao dispositivo inteligente.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_ Internet das Coisas no quotidiano_O3_O2:

Situação: Para ser um super-agente de cibersegurança, o que se deve fazer?

Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- a) Aprender a programar de modo a encriptar dispositivos IoT.
- b) Estabelecer um plano contingente seguindo os 4 Q's: "O que está a ser gerado?", "Onde são armazenados os dados?", "Quando são utilizados os dados?", e "Com quem são partilhados os dados?"
- c) Estabelecer um plano de contingência seguindo os 4 Q's: "A quem chamar?" "Qual é a minha linha de acção?", "Quando alertar os outros?", e "Quais actividades são incidentes?"
- d) Envolver toda a família, pares e funcionários na consciência da cibersegurança.
- e) Desenvolver o plano de resposta à incidência apenas depois de sofrer uma quebra de segurança, como é a única forma de conhecer as ações certas para os incidentes ainda por vir.



Fontes

Analytics Vidhya (26 Agosto 2016). *10 Real World Applications of Internet das Coisas (IoT) – Explained in Videos*. Retirado de <https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/>

Clark, J. (17 Novembro 2016). *What is the Internet das Coisas (IoT)?* Retirado de <https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/>

Evans, D. (2011). *The Internet das Coisas how the next evolution of the internet is changing everything*. Cisco White Paper, 1–11. Retirado de https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Griffiths, J. (2 Fevereiro 2019). *'Internet das Coisas' or 'vulnerability of everything'? Japan will hack its own citizens to find out*. Retirado de <https://edition.cnn.com/2019/02/01/asia/japan-hacking-cybersecurity-iot-intl>

Kelbert, J. (24 Setembro 2019). *5 Interesting Facts About the IoT*. Retirado de <https://blog.flexis.com/5-interesting-facts-about-the-internet-of-things-iot>

Mena, D. M., Papapanagiotou, I. and Yang, B. (2018) *Internet das Coisas: Survey on security*. Information Security Journal: A Global Perspective, 27:3, 162-182, DOI: 10.1080/19393555.2018.1458258

Finance Monthly (5 Setembro 2019). *The Worst And Weirdest IoT Hacks Of All Times*. Retirado de <https://www.finance-monthly.com/2019/09/the-worst-and-weirdest-iot-hacks-of-all-times/>

Ngo, D. (22 Dezembro 2015). *Home networking explained, part 9: Access your home computer remotely*. Retirado de <https://www.cnet.com/how-to/home-networking-explained-part-9-access-your-home-computer-remotely/>

Oorschot, P. C and Smoth, S. W. (2019). *The Internet das Coisas: Security Challenges*. IEEE Security and Privacy Magazine, 17(5):7-9. DOI: 10.1109/MSEC.2019.2925918

Spencer, T. (8 Agosto 2019). *How to Respond to a Cyber Attack*. Retirado de <https://www.industryweek.com/sponsored/article/22028042/how-to-respond-to-a-cyber-attack>

Viriati, M. S. et al. (2018). *Security and Privacy Challenges in Internet of Things*. Proceedings of the 2nd International Conference on Trends in Electronics and Informatics. IEEE Conference Record: # 42666; IEEE Xplore ISBN:978-1-5386-3570-4

Para lembrar

A **Internet das Coisas**, ou simplesmente IoT, é um chavão hoje em dia. A Internet das Coisas irá, sem dúvida nenhuma, mudar a forma como as pessoas interagem com o mundo e com a tecnologia à sua volta. Além disso, esta **rede de dispositivos ligados à Internet** terá muitos impactos positivos.

A IoT representa uma revolução na forma como interagimos uns com os outros. De facto, a IoT criou novos tipos de interação, uma vez que é **uma tecnologia que permite a ligação entre coisas, processos, pessoas, animais e quase tudo o que vemos à nossa volta, através da Internet**.



Co-funded by the
Erasmus+ Programme
of the European Union

Apesar de ser um conceito simples, a Internet das Coisas precisa de ter uma arquitetura complexa para funcionar corretamente. A arquitetura da IoT deve ser composta por, pelo menos, **quatro camadas**, nomeadamente: camada de percepção, camada de rede, camada de processamento e camada de aplicação. É nesta última camada que temos a percepção da utilidade da IoT, pois representa aplicações e dispositivos '*smart*' que podem ser utilizados em muitas áreas, tornando-os "mais inteligentes": casas inteligentes, agricultura inteligente, cidades inteligentes, cuidados de saúde inteligentes e muitos outros.

A dinâmica, inteligência e mobilidade da IoT fazem dela uma tecnologia com elevada procura mas também a tornam **vulnerável e arriscada em termos de segurança e privacidade**. Todas as camadas da IoT podem ser sujeitas a diferentes ciberataques. Portanto, **os designers de dispositivos inteligentes devem participar ativamente no desenvolvimento de medidas eficazes de segurança e privacidade**, tornando assim a IoT mais robusta em termos de segurança.

No entanto, a principal causa da vulnerabilidade da IoT é a **falta de sensibilização para a segurança**. As pessoas, as empresas e a sociedade em geral devem empenhar-se para melhorar os seus conhecimentos relacionados com a área de cibersegurança, a fim de eliminar a causa número um das violações da cibersegurança: o erro humano.

Lembra-te sempre, sê um superagente de Segurança Cibernética!



As respostas corretas estão assinaladas a negrito

Situação: O que é a “Internet das Coisas”?

Tarefa: Escolher a opção correta usando o princípio da escolha única: apenas uma resposta é verdadeira.

- A IoT é uma rede de servidores conectados que podem ser acedidos através da Internet.
- A IoT é a digitalização e automatização de cada parte de uma empresa, bem como do processo de fabrico.
- A IoT é uma rede global que liga sistemas informáticos em todo o mundo.
- **A IoT é uma tecnologia incipiente que se concentra na interligação entre coisas ou dispositivos uns aos outros e aos seres humanos ou utilizadores para atingir alguns objetivos comuns.**

Situação: Quais são as principais aplicações da Internet das Coisas?

Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- **Monitorização da linha elétrica e transição inteligente de energia da rede.**
- **Gestão da cadeia de fornecimento de produção no retalho.**
- **Gestão da cadeia de abastecimento da produção na indústria transformadora.**
- **Regulação da água na agricultura.**

Situação: No que toca à segurança dos dispositivos IoT e seus utilizadores, qual das afirmações é verdadeira?

Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- **A segurança dos dados é necessária quando os dados estão a ser gerados e armazenados.**
- Os requisitos de segurança para aplicações de IoT devem ser aplicados em três camadas: camada de aplicação, camada de rede e camada de perceção.
- A probabilidade de ocorrer um ataque de *phishing* num dispositivo IoT é maior na camada de processamento.
- **A arquitetura da IoT permite que entidades maliciosas explorem vulnerabilidades intrínsecas a cada uma das camadas da IoT.**
- **Um código malicioso pode afetar pelo menos três camadas.**

Situação: Considerando a privacidade dos utilizadores da IoT, qual das seguintes afirmações é verdade?

Tarefa: Escolher a opção correta usando o princípio da escolha única: apenas uma resposta é verdadeira.

- O crescimento significativo que a IoT tem mostrado durante os últimos anos trouxe várias preocupações de privacidade à medida que a disponibilidade de dados diminui, patrocinada pelas propriedades comuns e habituais da IoT.
- **Os fabricantes precisam de garantir a proteção das informações pessoais associadas aos movimentos, hábitos e interações dos utilizadores.**
- A privacidade refere-se à forma como os dispositivos da IoT se defendem contra o roubo de dados dos utilizadores.
- A privacidade só está em risco na camada da aplicação.



Situação: Quais as medidas de segurança que devemos implementar para evitar ciberataques nos dispositivos IoT?

Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- a) Instalar a encriptação homomórfica.
- b) Instalar *firewalls*.
- c) Criar dispersão de fragmentos redundantes.
- d) Alterar as palavras-passe pré-definidas do router.**
- e) Desativar funcionalidades no dispositivo inteligente que não estão a ser utilizadas.**
- f) Desativar o acesso remoto ao dispositivo inteligente.**

Situação: Para ser um superagente de cibersegurança, o que se deve fazer?

Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- a) Aprender a programar de modo a encriptar dispositivos IoT.
- b) Estabelecer um plano contingente seguindo os 4 Q's: "O que está a ser gerado?", "Onde são armazenados os dados?", "Quando são utilizados os dados?", e "Com quem são partilhados os dados?"
- c) Estabelecer um plano de contingência seguindo os 4 Q's: "A quem chamar?" "Qual é a minha linha de ação?", "Quando alertar os outros?", e "Quais atividades são incidentes?"**
- d) Envolver toda a família, pares e funcionários na consciência da cibersegurança.**
- e) Desenvolver o plano de resposta à incidência apenas depois de sofrer uma quebra de segurança, como é a única forma de conhecer as ações certas para os incidentes ainda por vir.