FACULDADE DE TECNOLOGIA E CIÊNCIAS SOCIAIS APLICADAS – FATECS

ENGENHARIA DA COMPUTAÇÃO

MARCUS VINÍCIUS CÂNDIDO DE PAULA

21706888

SEGURANÇA DA INFORMAÇÃO E A INTERNET DAS COISAS

BRASÍLIA

2020

MARCUS VINÍCIUS CÂNDIDO DE PAULA

SEGURANÇA DA INFORMAÇÃO E A INTERNET DAS COISAS

Trabalho de Conclusão de Curso (TCC) apresentado como um dos requisitos para a conclusão do curso de Engenharia de Computação do UniCEUB– Centro Universitário de Brasília

Orientador (a): Prof. MsC Francisco Javier de Obaldía Díaz

BRASÍLIA

2020

MARCUS VINÍCIUS CÂNDIDO DE PAULA

SEGURANÇA DA INFORMAÇÃO E A INTERNET DAS COISAS

Trabalho de Conclusão de Curso (TCC) apresentado como um dos requisitos para a conclusão do curso de Engenharia de Computação do UniCEUB – Centro Universitário de Brasília

Orientador (a): Prof. MsC Francisco Javier de Obaldía Díaz

Brasília, 2020.

BANCA EXAMINADORA

_____

Professor MsC. Francisco Javier de Obaldía Díaz

Orientador

_____

Professor MsC. Ivandro da Silva Ribeiro

Examinador

_____

Professor MsC. Ricardo Alves Moraes

Examinador

SEGURANÇA DA INFORMAÇÃO E A INTERNET DAS COISAS
INFORMATION SECURITY AND THE INTERNET OF THINGS

Marcus Vinícius Cândido de Paula[1], Professor MsC. Francisco Javier de Obaldía Díaz[2], Professor MsC. Ivandro da Silva Ribeiro[3], Professor MsC. Ricardo Alves Moraes[4]

RESUMO. Tem ocorrido um aumento impressionante dos investimentos e uso de dispositivos e plataformas de Internet das Coisas (*Internet of Things*, IoT). De assistentes pessoais a monitores cardíacos, de geladeiras a fechaduras inteligentes, todos eles conectados à internet, com o objetivo de facilitar a vida das pessoas. Todo esse crescimento traz uma preocupação com a segurança dos dados pessoais nesse ecossistema. Mesmo com várias leis, *frameworks* e regulamentações para proteção de dados, tem-se, todos os anos, muitos incidentes de segurança envolvendo IoT. Nesse artigo, será contemplada a segurança da informação pelos olhos da Lei Geral de Proteção de Dados (LGPD, Brasil), a *General Data Protection Regulation* (GDPR, Europa) e o Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards and Technology* – NIST, Estados Unidos) e seus *frameworks*, com foco em IoT. Aspectos de ciber-segurança e proteção serão abordados e comparados com três recentes falhas de segurança ocorridas no universo IoT, mostrando que, observando apenas as leis, *frameworks* e regulamentações já existentes, muitas das falhas seriam evitadas.

"O que *a IoT significa para mim é: dispositivos inteligentes que trazem os riscos e ameaças que sempre vimos na indústria e sistemas de controle digital, para dentro do dia a dia de* pessoas reais." REITINGER, Philip, Global Cyber Alliance (Tradução nossa)

Palavras-chave: Segurança. Internet. Privacidade.

Abstract: There has been an impressive growth in investments and use of Internet of Things (IoT) devices and platforms. From personal assistants to cardiac monitors, from smart refrigerators to smart locks, all connected to the internet, with the aim of making people's lives easier. All this growth brings a concern with the security personal data in this ecosystem. Even with various laws, frameworks and regulations for data protection, there are still many security incidents involving IoT. In this article, we will look at information security through the eyes of the General Data Protection Law (*Lei Geral de Proteção de Dados* – LGPD, Brazil), the General Data Protection Regulation (GDPR, Europe) and the National Institute of Standards and Technology (NIST, United States) and its frameworks, focused on IoT. Aspects such as cybersecurity data protection will be addressed and compared with three recent security flaws in the IoT universe, showing that by observing only existing laws, frameworks, and regulations, many of the failures would be avoided.

"What IoT means to me is: intelligent smart devices that br*ing the risks and threats that we have always seen in the industrial and digital control system space, into the lives of real people."* REITINGER, Philip, Global Cyber Alliance

Keywords: Security. Internet. Privacy.

[1] UniCEUB, aluno.
[2] UniCEUB, orientador.
[3] UniCEUB, primeiro examinador.
[4] UniCEUB, segundo examinador.

1. INTRODUÇÃO

Com milhões ou até bilhões de dispositivos conectados à internet nos próximos anos, como será possível manter a privacidade e a segurança de todos os dados pessoais que serão acessados ou armazenados por eles?

Esses dispositivos estão cada dia mais presentes nas vidas das pessoas, e com isso, têm-se acesso a mais informações pessoais e de sua privacidade.

Nos últimos anos, tem acontecido uma corrida por leis, regulamentações e *frameworks* para proteção de dados pessoais e ciber-segurança. No caso dos *frameworks*, eles contêm várias publicações com melhores práticas, voltadas para organizações, fabricantes de dispositivos e serviços, inclusive publicações específicas sobre IoT.

Com um maior foco nos dados pessoais, no Brasil, em 2020, entrou em vigor a Lei Geral de Proteção de Dados (LGPD) e na União Europeia, entrou em vigor em 2018 a *General Data Protection Regulation* (GDPR), que foi, em certos aspectos pioneira no que diz respeito à proteção de dados pessoais. Nos Estados Unidos, além de várias leis de proteção de dados em vigor, tem-se o *National Institute of Standards and Techonology* (NIST), com seus *frameworks*.

Como pode-se ver, existem várias formas de especificar e regulamentar ciber-segurança para dispositivos da IoT, que sejam seguros o suficiente e que não coloquem informações pessoais ou sensíveis em risco.

Essa preocupação é justificada, pois os números atuais e as previsões de investimentos e utilização de dispositivos e plataformas IoT são impressionantes.

Algumas das previsões relacionadas a IoT falam em 41 bilhões de dispositivos até 2027; até 2023, 70% dos automóveis estarão conectados à Internet; a cada segundo, 127 novos dispositivos estão conectados à Internet; até 2024, haverá 1,9 bilhão de celulares 5G; empresas vão investir cerca de U$ 1.1 Trilhão de dólares em IoT até 2023; até 2025 o impacto total da IoT na economia dever ser entre U$ 4 e U$ 11 Trilhões de dólares por ano; o mercado residencial de IoT deve crescer para mais de U$ 53 Bilhões de dólares; até 2024, o mercado global de IoT na Saúde deve alcançar U$ 140 Bilhões de dólares; mais de 80% das indústrias de manufatura planejam usar ou já usam dispositivos IoT; nove de dez executivos de Tecnologia, Mídia e Telecomunicações dizem que o crescimento da IoT é crítico para seus negócios; 60% das cidades nos Estados Unidos estão investindo em tecnologias IoT para cidades inteligentes; quase 90%dos varejistas estão usando ou planejam usar IoT para customizar as visitas às suas lojas. (VXGHNGE, 2020)

Com todos esses investimentos e previsões para esse mercado, é preciso que a indústria de IoT esteja cada vez mais atenta e comprometida com a segurança dos dados transmitidos ou armazenados em seus produtos e serviços. Esse estudo será focado na segurança da informação das casas inteligentes (automação residencial) e cidades inteligentes.

2. REFERENCIAL TEÓRICO

2.1 INTERNET DAS COISAS – *INTERNET OF THINGS (IOT)*

Quando, em 1999, Kevin Anston utilizou pela primeira vez o termo Internet das Coisas (*Internet of Things)*, provavelmente ele não imaginava que ele seria usado para identificar bilhões de dispositivos ao redor do mundo. Kevin criou padrões globais para o *Radio-frequency Identification* (RFID) e outros

sensores. O termo foi usado por ele inicialmente para descrever um sistema onde a Internet estaria conectada ao mundo físico através de sensores. (FINEP, 2015)

A primeira implementação conhecida de IoT foi no início dos anos 1980, quando um grupo de estudantes da Universidade Carnegie Mellon conseguiu monitorar uma máquina de venda de bebidas, verificando a quantidade de refrigerante ainda disponível na máquina.

David Nichols, um estudante de graduação do departamento de Ciências da Computação, estava em seu escritório, desejando um refrigerante. Era uma distância relativamente longa do escritório até a máquina de refrigerantes, e ele ainda correria o risco de ela estar vazia ou ter sido reabastecida recentemente (nesse último caso, os refrigerantes ainda estariam quentes. Então Nichols falou sobre sua ideia com alguns amigos e, logo dois outros estudantes – Mike Kazar e Ivor Durham – e um pesquisador de Engenharia, John Zsarnay, começaram a trabalhar com Nichols. (IBM, 2018)

Para conseguir determinar a quantidade de refrigerantes na máquina à distância, era preciso monitorar suas luzes. A máquina tinha 6 colunas com garrafas de refrigerante. Quando alguém comprava um, uma luz vermelha na coluna correspondente acenderia por alguns segundos e depois desligaria. Quando alguma coluna estivesse vazia, a luz continuaria acesa até que a máquina fosse reabastecida.

Zsarnay instalou uma placa que, através de um sensor, identificaria o status de cada luz da máquina, essa placa estava conectada ao computador central do departamento, que por sua vez estava conectado a ARPANET, rede precursora a Internet, que nessa época, conectava cerca de 300 computadores espalhados pelo mundo.

Kazar escreveu um programa que checava o status de cada luz algumas vezes por segundo. Se uma luz mudasse de desligada para ligada, mas depois desliga-se novamente alguns segundos depois, ele saberia que um refrigerante havia sido comprado. Se uma luz ficasse ligada por mais de cinco segundos, o programa consideraria que aquela coluna estava vazia. Quando essa luz voltasse a desligar, o programa saberia que dois refrigerantes gelados – que sempre eram mantidos como reserva – estariam então disponíveis para venda, enquanto o restante das garrafas estaria quente. O programa registrava a quantos minutos os refrigerantes estavam na máquina depois delas serem reabastecidas. Assim, depois de três horas, as garrafas eram consideradas geladas.

Depois, o grupo incluiu um código ao computador central, que permitiu que qualquer um, com o computador conectado na ARPANET ou na rede local da universidade, poderia acessar as informações sobre a máquina.

"Eu nunca usei, exceto para ver se estava funcionando. Eu nunca gostei de Coca-Cola" (Tradução nossa). Kazar, Mike, Estudante da Universidade Carnegie Mellon.

De acordo com Kazar, devido à grande quantidade de máquinas de refrigerantes na universidade, o programa se tornou popular bem rapidamente no departamento de computação, quando ele se tornou operacional em 1982. Com o tempo, se tornou comum verificar o status da máquina antes de sair. Todos queriam garantir que conseguiriam o refrigerante mais gelado disponível. Depois disso, outro estudante montou um sistema similar, desta vez para monitorar o status de uma máquina de M&M[5] próxima. (IBM, 2018)

Esse grupo de estudantes certamente não imaginava que aquela

[5] Marca pertencente a *Mars, Incorporated* que se refere principalmente a pequenos pedaços de chocolate ao leite recobertos por uma camada de açúcar.

máquina de bebidas seria a primeira de bilhões de dispositivos conectados à Internet. Atualmente, se estima que temos mais de trinta bilhões deles. Dispositivos IoT estão por todo lugar, desde celulares a monitores cardíacos em relógios, de assistentes pessoais a automação industrial, câmeras monitoram todos seus passos, carros, geladeiras, cafeteiras e vários outros utensílios do nosso dia-a-dia podem ser encontrados em sua versão "inteligente", conectada à rede mundial de computadores (ou seria de dispositivos?).

2.2 A *GENERAL DATA PROTECTION REGULATION* (GDPR)

Em 14 de Abril de 2016, foi criada a *General Data Protection Regulation* – Regulação Geral de Proteção de Dados – a GDPR é uma Lei de proteção de dados e privacidade vigente em toda União Europeia e Área Econômica Europeia. Ela também aborda a transferência de dados pessoais para fora dessas áreas. O objetivo da GDPR é dar controle aos indivíduos sobre seus dados pessoais e simplificar a regulação para negócios internacionais, isso foi alcançado unificando a regulação dentro da União Europeia.

A GDPR, que entrou em vigor em 25 de Maio de 2018, foi precursora na proteção de dados pessoais e foi alicerce para várias outras leis criadas em seguida, inclusive a Lei Geral de Proteção de Dados, a LGPD, criada no Brasil em 14 de Agosto de 2018.

"O Regulamento Geral de Proteção de Dados (GDPR) é a lei de privacidade e segurança mais rígida do mundo. Embora tenha sido redigido e aprovado pela União Europeia (UE), ele impõe obrigações a organizações em qualquer lugar, desde que visem ou coletem dados relacionados a pessoas na UE. O regulamento entrou em vigor em 25 de maio de 2018. O GDPR aplicará multas severas contra aqueles que violarem seus padrões de privacidade e segurança, com penalidades que podem chegar a dezenas de milhões de euros." (GDPR.EU, 2018) (Tradução nossa)

Com relação a quem processa dados pessoais (controladores), a GDPR exige que sejam respeitados sete princípios:

1. L**egalidade, justiça e transparência –** o processamento deve ser legal, justo e transparente para o titular dos dados.
2. **Limitação de Finalidade –** os dados devem ser processados somente para os fins explicitamente especificados para o titular dos dados quando foram coletados.
3. **Minimização de dados –** coletar e processar somente os dados absolutamente necessários para os fins especificados.
4. **Precisão –** os dados pessoais devem ser mantidos precisos e atualizados.
5. **Limitação de armazenamento –** os dados de identificação pessoal podem ser armazenados somente pelo tempo necessário para a finalidade especificada.
6. **Integridade e confidencialidade –** a segurança, integridade e confidencialidade adequadas dos dados pessoais devem ser garantidos durante o processamento.
7. **Responsabilidade –** o controlador (quem processa e armazena os dados) é responsável por demonstrar conformidade com todos esses princípios.

Além desses princípios, que devem ser obedecidos pelos que controlam e processam os dados pessoais, a GDPR lista oito direitos dos titulares dessas informações:

1. **O direito de ser informado –** o titular tem o direito de solicitar ao controlador quais informações e para quais finalidades foram coletadas.
2. **O direito de acesso –** o titular tem o direito de acessar os dados que foram coletados, assim como solicitar cópias deles.
3. **O direito de retificação –** o titular tem o direito de pedir alterações nos dados coletados, caso acredite que eles não estejam precisos ou atualizados.
4. **O direito de retirar o consentimento –** o titular pode optar por remover um consentimento prévio para processamento de seus dados.
5. **O direito de remoção -** (‘direito de ser esquecido’) o titular tem o direito de solicitar que seus dados pessoais sejam apagados, usualmente ocorre ao fim do relacionamento com o controlador.
6. **O direito de restringir o processamento –** similar a retirada de consentimento, o processamento dos dados pode ser interrompido, a pedido do titular, quando uma disputa judicial com o controlador está em andamento.
7. **O direito à portabilidade dos dados –** o titular pode solicitar a transferência de seus dados, para si mesmo ou para outro controlador.
8. **Direitos em relação à tomada de decisão automatizada e definição de perfis –** o titular tem o direito de não aceitar uma decisão, baseada em seus dados pessoais, tomada de forma automatizada. Nesse caso, essa decisão deve ser revisada manualmente.

“Vivemos em uma *era em que os dados valem ouro. Na verdade, qualquer pessoa que opere no espaço da IoT deve estar ciente das recentes mudanças no programa de proteção de dados da União Europeia.”* (Atoui, Roland[6], 2019). (Tradução nossa)

2.3 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Aprovada em 14 de Agosto de 2018, a Lei 13.709, Lei Geral de Proteção de Dados Pessoais foi criada para regulamentar o tratamento de dados pessoais e tem como fundamentos: proteger a privacidade, autodeterminação informativa, liberdade de expressão, de informação, de comunicação e de opinião, inviolabilidade da intimidade, da honra e da imagem, desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor, os direitos humanos, o livre desenvolvimento da personalidade e o exercício da cidadania pelas pessoas. Ela deve ser seguida em todas as situações em que os dados pessoais sejam coletados e/ou tratados dentro do território nacional – nesse caso, o titular das informações precisa estar em território nacional[7]. (LGPD, 2018)

[6] Roland Atoui é um especialista em segurança cibernética e Internet das Coisas (IoT), com reconhecidas realizações trabalhando para empresas como Gemalto e Oracle, com experiência em pesquisa e indústria.

[7] Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019.

A LGPD, que entrou em vigor em 18 de Setembro de 2020, e foi fortemente baseada na regulamentação Europeia para os mesmos fins, a *General Data Protection Regulation* (GDPR), as duas tem bastante em comum, sendo que a GDPR é mais rígida, tanto na proteção dos dados quanto nas punições aos que não a cumprirem.

A LGPD é uma Lei bastante abrangente e complementa o Marco Civil da Internet[8], mas alguns aspectos dela estão mais conectados ao universo da IoT:

- **Coleta dos Dados**: deve haver consentimento expresso do titular (pessoa a quem os dados se referem) sobre a coleta, o uso, o armazenamento e a proteção dos dados pessoais. Os dados devem ser permanentemente excluídos assim que concluída a relação entre as partes e a pedido do titular, salvo quando está previsto em lei algum tipo de guarda obrigatória desses dados.
- **Proteção dos Dados**: devem ser preservadas a intimidade, a vida privada, a honra e a imagem das partes direta e indiretamente envolvidas. Os provedores de serviços relacionados a internet devem permitir a checagem das medidas tomadas para o cumprimento da LGPD quanto aos seguintes aspectos: coleta, guarda, armazenamento, tratamento dos dados, além da privacidade e sigilo das comunicações.
- **Sanções Administrativas**: Em casos de não cumprimento da lei, os agentes de tratamento de dados podem ser alvo de algumas penalidades (de forma isolada ou cumulativa): advertência, com prazo para aplicar as correções necessárias; multa de até 2% (dois por cento) do faturamento da empresa no último ano, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; multa diária até que o problema seja resolvido, publicização[9] da infração após apuração e confirmação de sua ocorrência, bloqueio dos dados pessoais a que se refere a infração até que esta seja regularizada, eliminação dos dados pessoais a que se refere a infração, suspensão parcial do banco de dados a que se refere a infração, suspensão das atividades de tratamento de dados a que se refere a infração por até 6 (seis) meses, prorrogável por igual período e proibição parcial ou total das atividades de tratamento de dados.
- **Divulgação de Incidentes de Segurança**: no caso de incidentes de segurança que possam acarretar riscos ou danos aos titulares, tanto a autoridade nacional[10] quanto o titular (ou titulares) deverão ser comunicados o mais rapidamente possível sobre o ocorrido. Nessa comunicação, devem constar, obrigatoriamente: descrição dos dados pessoais afetados, titulares envolvidos, medidas técnicas e de segurança utilizadas para a proteção dos dados, riscos relacionados ao incidente, motivos da demora na comunicação (quando esta não ocorrer em tempo razoável) e as medidas tomadas para resolução ou mitigação do incidente.

Especificamente com relação as cidades inteligentes, temos um outro aspecto a ser considerado; a participação do governo:

- **Tratamento dos dados pessoais pelo poder público**: quando o governo em geral é o agente de tratamento de dados,

[8] Lei nº 12.965, 23 de Abril de 2014, Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

[9] Divulgação; ação de fazer com algo se torne público; realizar publicidade. Mudança da administração de serviços públicos que passam para o domínio particular, sendo seu financiamento responsabilidade do poder executivo. [Jurídico] Intervenção legislativa em setores que fazem parte do âmbito privado.

[10] A autoridade nacional é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta (LGDP e Marco Civil da Internet) em todo o território nacional. Lei Nº 13.709, 14 de Agosto de 2018. Artigo 2º, XIX.

esse tratamento deverá ter finalidade pública, buscar o interesse público e ter como objetivo apenas executar e cumprir as competências e atribuições legais do serviço público. Isso deve ser feito de acordo com algumas regras: é necessário que sejam divulgadas de forma clara e sempre atualizadas, informações sobre a previsão legal para o uso dos dados, a finalidade, os procedimentos e práticas usados no tratamento dos dados e, além disso, um Encarregado[11] deve ser indicado para essas operações.

2.4 O *NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY* (NIST)

O *National Institute of Standards and Technology* (NIST) foi fundado em 1901 e faz parte do Departamento de Comércio dos Estados Unidos.

Desde redes elétricas inteligentes e registros médicos eletrônicos, até relógios atômicos, chips de computadores e segurança da informação, vários produtos e serviços dependem de alguma forma de tecnologia, medição e padrões fornecidos pelo NIST.

No que diz respeito a Segurança da Informação, o NIST iniciou em 2013, dentro do *National Cybersecurity Center of Excellence (NCCoE)*[12], o desenvolvimento do seu *Cybersercurity Framework*. Ele é um *framework* voluntário, baseado em padrões, diretrizes e melhores práticas já existentes até então, com o objetivo de reduzir os riscos de segurança em infraestruturas críticas. O *framework* foi criado com a colaboração da indústria e o governo.

> *"Aqui, no NCCoE, National Cybersecurity Center of Excellence; indústria, governo e academia trabalham lado a lado desenvolvendo soluções práticas para alguns dos desafios de segurança cibernética mais urgentes da indústria." (NIST, 2018)* (Tradução nossa)

Em 2016, também nos Estados Unidos, foi criado o *Cybersecurity for IoT Program*, com o desafio de promover a ciber-segurança para dispositivos e dados no ecossistema IoT, por todos os setores da indústria e em escala. A missão desse programa é de que cultive a confiança na IoT e promova um ambiente que permita a inovação em escala global por meio de padrões, diretrizes e ferramentas relacionadas.

Duas publicações do NIST, recentemente atualizadas (Maio/2020) e concebidas dentro do *Cybersecurity for IoT Program*, foram a NISTIR 8259 - *Foundational Cybersecurity Activities for IoT Device Manufacturers* (Atividades básicas de ciber-segurança para fabricantes de dispositivos IoT) e a NISTIR 8259A - *IoT Device Cybersecurity Capability Core Baseline* (Linha de base principal da capacidade de ciber-segurança do dispositivo IoT).

A NISTIR 8259 tem como objetivo dar recomendações de práticas de ciber-segurança que os fabricantes deveriam realizar antes de colocar seus produtos à venda. São seis melhores práticas recomendadas, executadas tanto na pré-venda quanto na pós-venda. (NIST, 2020)

- Prática 1: **Identifique clientes e usuários esperados e definir casos de uso –** com essas informações é possível, no começo do

[11] O Encarregado pelo tratamento de dados pessoais será responsável por determinada operação, interagindo com os titulares, autoridade nacional, além de funcionários e contratados da entidade. Lei Nº 13.709, 14 de Agosto de 2018. Artigo 41º.

[12] O NCCoE, Centro Nacional de Excelência em Ciber-segurança, é uma parceria público privada que permite a criação de soluções práticas de segurança cibernética para setores específicos, bem como para desafios tecnológicos abrangentes e intersetoriais.

desenvolvimento do produto, determinar quais itens de segurança seriam implementados e como eles seriam implementados;

- Prática 2: **Pesquise as necessidades e objetivos de segurança dos clientes e usuários –** os fabricantes podem produzir seus dispositivos de forma que possam ser minimamente seguros com ações de seus clientes, usuários e casos de uso;
- Prática 3: **Determine como atender as necessidades e objetivos dos usuários e clientes –** isso pode ser cumprido atendendo práticas da publicação NIST 8259A, provendo condições para ajudar os clientes e usuários a mitigar seus riscos de segurança;
- Prática 4: **Planeje o suporte adequado às necessidades e objetivos dos clientes e usuários –** para tornar seus dispositivos mais seguros, os fabricantes podem prover recursos adequados de hardware e software do dispositivo, para oferecer suporte aos recursos de ciber-segurança desejados. Além disso, devem considerar os recursos de negócios necessários para apoiar o desenvolvimento e o suporte contínuo do dispositivo IoT;
- Prática 5: **Defina abordagens de comunicação com os clientes e usuários** - Muitos se beneficiarão com a comunicação mais clara dos fabricantes sobre os riscos de ciber-segurança envolvendo os dispositivos IoT que os fabricantes estão vendendo ou já venderam,
- Prática 6: **Defina o que comunicar aos clientes e usuários, e como comunicá-los –** essa comunicação pode variar bastante, e o NIST cita alguns exemplos de tópicos a serem analisados: suposições relacionadas aos riscos de segurança feitas pelo fabricante; expectativas de suporte e vida útil do produto; composição e recursos do dispositivo; as atualizações software; informações sobre retirada de circulação e recursos de segurança oferecidos pelo dispositivo e serviços relacionados.

Já a NIST 8259A, visa fornecer um ponto de partida para que a indústria em geral possa identificar requisitos mínimos de segurança em dispositivos IoT que serão fabricados, integrados ou adquiridos por ela. A definição desses requisitos mínimos de segurança é feita através de uma tabela, com informações sobre o recurso a ser considerado, como a identificação do dispositivo; seguido de uma lista de elementos do recurso, identificador único e identificador físico; uma justificativa para a implementação, que explica porque aquele requisito deve ser cumprido, e referências para recursos similares, vindos de outras entidades e associações que tratam de ciber-segurança.

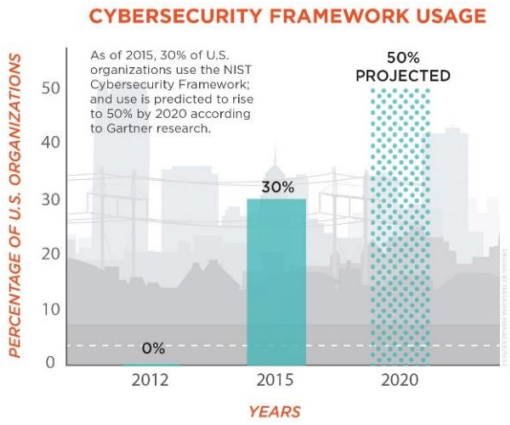
Os padrões, diretrizes e melhores práticas do NIST são cada vez mais utilizados, nos Estados Unidos, dezesseis setores críticos de infraestrutura e vinte estados adotaram o *framework.* (TELES, Guilherme, 2020).

As publicações do NIST também foram traduzidas para vários idiomas, isso se reflete no uso delas por governos de outros países, como Japão e Israel.

A Figura 1 mostra uma projeção do número de organizações que utilizam o *Cybersecurity Framework*, fazendo uma comparação entre os anos de 2012, quando não havia adesão, 2015, já com 30%, e uma projeção de 50% das organizações dos Estados Unidos adotarem o *framework* do

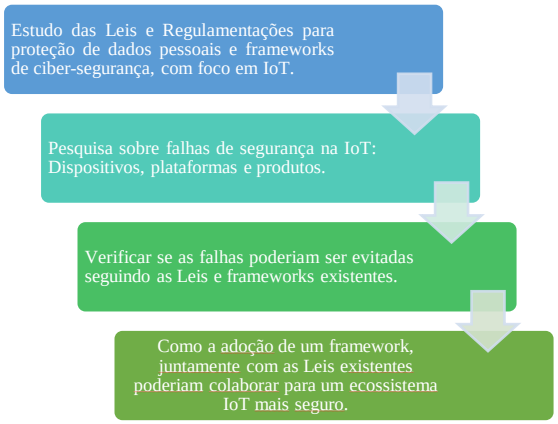
NIST até o final de 2020. A pesquisa foi realizada pelo instituto Gartner[13], em 2017.

Figura 1: Uso do *framework* de segurança do NIST.



Fonte: Gartner, 2017.

Figura 2: Metodologia utilizada no estudo.



Fonte: Autor.

3. METODOLOGIA

Nesse estudo, com o objetivo de demonstrar que com as leis, regulamentações e *frameworks* existentes, poderia se evitar grande parte dos incidentes de segurança envolvendo dispositivos IoT, foi feito uma análise de duas leis (ou regulamentações), a LGPD e a GDPR, e dos *frameworks* do NIST voltados para ciber-segurança da IoT. Além disso, foi feita uma pesquisa sobre falhas de segurança recentes envolvendo dispositivos IoT de casas e cidades inteligentes.

Com a descrição das falhas e suas causas chega-se à conclusão de que com a adoção de um *framework* de segurança e obediência às leis existentes, os fabricantes e desenvolvedores de dispositivos e plataformas para IoT, cooperariam para que esse ecossistema fosse bem mais seguro e confiável.

Na Figura 2, observa-se um resumo da metodologia utilizada nesse estudo.

4. ANÁLISE E RESULTADOS

4.1 IOT E AS CIDADES INTELIGENTES

As pessoas continuam se mudando para as grandes cidades, isso se deve principalmente às oportunidades de emprego, estilo de vida, cultura e assim por diante.

Por conta desse aumento populacional nos grandes centros, essas cidades precisam se tornar mais eficientes, e é nesse momento que entra o conceito de cidades inteligentes.

De acordo com a Cisco Systems, "*uma cidade inteligente usa tecnologia digital para conectar, proteger e melhorar a vida dos cidadãos. Sensores de IoT, câmeras de vídeo, redes sociais e outros meios de entrada, agem como um sistema nervoso, provendo os operadores da cidade e aos cidadãos atualizações constantes para que possam tomar decisões*

[13] Fundado em 1979, o Gartner é a empresa líder em pesquisa e consultoria. Eles se expandiram muito além de sua principal pesquisa de tecnologia para fornecer aos líderes seniores em toda a empresa os insights de negócios indispensáveis, conselhos e ferramentas de que precisam para alcançar suas prioridades de missão crítica e construir as organizações de amanhã.

informadas. Uma cidade inteligente coleta e analisa dados dos sensores IoT e câmeras de vídeo. Ela "sente" o ambiente de forma que o operador possa decidir como e quando agir. Algumas ações podem ser realizadas automaticamente. Por exemplo, uma lixeira pública pode contactar o serviço de coleta quando sua capacidade estiver perto de ser atingida, ao invés de esperar pela coleta agendada." (Tradução nossa)

A Cisco também fala sobre alguns benefícios das cidades inteligentes:

- Para os cidadãos, há uma melhora na utilização diária dos serviços públicos. Com as cidades inteligentes há uma maior visibilidade do que acontece em tempo real, melhorando a mobilidade, conectividades e segurança dos cidadãos.
- Para os negócios, pode trazer um desenvolvimento econômico baseado nas atividades e comportamento dos cidadãos.
- Para os serviços públicos, as operações podem ser otimizadas e mais eficientes por conta das informações em tempo real providas pela IoT, além disso, uma maior participação dos cidadãos e maior colaboração entre as diferentes áreas dos serviços públicos.
- Para desenvolvedores e fabricantes, toda essa massa de dados estimula a criação de novas aplicações e dispositivos, o que ajudará a cidade a ter mais eficiência operacional, maior engajamento dos cidadãos e movimentar a economia.

Dentre as várias áreas impactadas com o conceito de cidades inteligentes, algumas se destacam:

- Eficiência energética
- Iluminação pública
- Estacionamento e abastecimento de veículos
- Trânsito
- Coleta de Lixo
- Segurança
- Saúde

Tudo isso ainda pode ser mais útil e trazer mais benefícios quanto mais integradas essas áreas se tornarem.

Mas com toda essa tecnologia e conectividade, vem os problemas de segurança. O que aconteceria se um agente malicioso conseguisse assumir o controle dos semáforos de uma dessas cidades? Ou então, 'sequestrando' as lixeiras inteligentes, as usasse para capturar informações dos cidadãos passantes, através de celulares, relógios ou carros inteligentes. Poderiam assumir o controle da iluminação pública, criando apagões em lugares estratégicos para cometerem outros crimes. A ciber-segurança desses dispositivos se faz imprescindível para evitar eventos como esses aconteçam.

4.2 IOT E A AUTOMAÇÃO RESIDENCIAL (CASAS INTELIGENTES)

O termo Automação residencial se refere ao controle automático de aparelhos eletrônicos de uma casa. Com a chegada de dispositivos IoT, esses aparelhos passaram a se conectar com a internet, podendo ser controlados remotamente. O termo mais usado atualmente é o de casas inteligentes.

De acordo com o Wikipedia, alguns tipos de dispositivos são mais comuns nas casas inteligentes:

- Controle de Iluminação
- Controle de Temperatura
- Segurança residencial
- Monitoramento de Energia
- Controle do trancamento de portas e janelas

- Irrigação do jardim ou quintal
- Eletrodomésticos inteligentes
- Detectores de fumaça, água e gás
- Sistemas integradores

4.3 INCIDENTES DE SEGURANÇA EM DISPOSITIVOS E SERVIÇOS DE IOT

A chegada da IoT e sua forte presença em nosso dia a dia, principalmente em cidades e casas inteligentes, trazem muito conforto, praticidade, eficiência e segurança. Mas por outro lado, também existem os desafios e problemas relacionados a segurança das informações coletadas e tratadas por todo o ecossistema de IoT.

Em 2019 ocorreram vários incidentes de segurança da informação envolvendo dispositivos e serviços IoT. Muitos desses incidentes poderiam ser evitados seguindo algumas das leis, normas e melhores práticas que destacamos anteriormente.

A Forbes, em Julho de 2019, publicou: "Confirmado: 2 bilhões de registros expostos em grande falha em dispositivo de casa inteligente". Os pesquisadores em segurança da informação, Noam Rotem e Ran Locar da empresa vpnMentor[14], descobriram que uma base de dados de uma empresa chinesa, Orvibo[15], poderia ser acessada pela internet, não havia nenhum tipo de segurança aplicada, nem mesmo uma senha. As coisas ficaram ainda piores quando descobriram que, nessa base de dados, havia mais de dois bilhões de registros contendo de senhas de usuários a um vídeo de uma câmera inteligente.

A lista de dados incluídos nessa base de dados é bem extensa, segundo o relatório da vpnMentor, e contém:

- Endereços de e-mail
- Senhas
- Códigos de reconfiguração de contas
- Geolocalização
- Endereço IP
- Nome de usuário
- Identificação de Usuário
- Nome da Família
- Identificação da Família
- Dispositivo inteligente
- Dispositivo que acessou a conta
- Informações de agendamento

Foram encontrados registros de usuários localizados em várias partes do mundo, como Brasil, China, Japão, Tailândia, México, França, Austrália, Reino Unido e Estados Unidos.

Como mencionado, uma das informações armazenadas da base de dados são os códigos de reconfiguração da conta do usuário, isso permitiria que os criminosos alterassem tanto a senha quanto o endereço de e-mail das contas, obtendo total controle sobre os dispositivos. Que no caso da Orvibo, vão de cadeados inteligentes a câmeras de segurança e sistemas completos para casas inteligentes.

Após a publicação do relatório, a Orvibo se pronunciou, através de seu porta-voz:

"Assim que recebemos este relatório em 2 de julho, a equipe de RD de Orvibo tomou medidas imediatas para resolver a vulnerabilidade de segurança e informou o repórter. Orvibo atribui grande importância à segurança dos dados do usuário e continua melhorando os sistemas de segurança da informação." (Tradução nossa)

O portal ZDNet, em Outubro de 2019, publicou: "Dispositivos Alexa e

[14] vpnMentor é uma empresa que fornece serviços de redes virtuais privadas (VPN).

[15] Orvibo é uma empresa chinesa, baseada em Shenzhen, que opera uma plataforma de gerenciamento de dispositivos para casas inteligentes.

Google Home são usados para roubar e espionar usuários, novamente". Sim, novamente. Os mesmos tipos de ataques já haviam ocorrido anteriormente tanto em dispositivos Alexa (Abril/2018 e Agosto/2018) quanto Google Home (Maio/2018).

Ambos os fabricantes tomaram as medidas necessárias depois de cada descoberta, mas os hackers sempre encontram uma nova forma de seguir bisbilhotando e enganando os usuários, fazendo com que entreguem dados sensíveis.

As falhas de 2019 foram identificadas no mesmo ano, por Luise Frerichs e Fabian Bräunlein, pesquisadores de segurança do Security Research Labs (SRLabs)[16]. Nos dois casos, Alexa e Google, o phishing[17] e a espionagem ocorrem através da plataforma disponibilizada pelos fabricantes para customização de aplicações. Os desenvolvedores têm a possibilidade de customizar comandos que os dispositivos vão atender e como eles vão responder esses comandos.

A equipe do SRLabs descobriu que, ao adicionar a sequência de caracteres "." (U + D801, ponto, espaço) a vários locais dentro de um aplicativo Alexa / Google Home original, eles poderiam induzir longos períodos de silêncio durante os quais o assistente permanece ativo. Com isso poderia se dizer ao usuário que um aplicativo falhou e então incluir o "." e depois da pausa enviar a mensagem de phishing, fazendo o usuário pensar que essa mensagem não está relacionada com o aplicativo anterior.

Esse tipo de ataque afeta os dois dispositivos e explora o fato de que os fabricantes somente verificam os aplicativos quando eles são submetidos da primeira vez, as atualizações seguintes não são verificadas.

Os dois fabricantes se pronunciaram após a divulgação das falhas:

"Todas as ações no Google devem seguir nossas políticas de desenvolvedor e proibimos e removemos qualquer ação que viole essas políticas. Temos processos de revisão para detectar o tipo de comportamento descrito neste relatório e removemos as ações que encontramos desses pesquisadores. Estamos implementando mecanismos adicionais para evitar que esses problemas ocorram no futuro. " Google. (Tradução nossa)

A Amazon disse a mesma coisa - que seus dispositivos nunca pediriam a senha de um usuário - e que eles *"aplicam medidas para prevenir e detectar esse tipo de comportamento e rejeitá-los ou retirá-los quando identificados"*. (Tradução nossa)

E não termina aí, segundo a ZDNet, depois da publicação do artigo, outros pesquisadores os procuraram para falar de outros novos métodos para incluir atos maliciosos nos dois dispositivos.

O portal Michigan News (Universidade de Michigan), em Maio de 2016, publicou: "Invadindo casas: falhas de segurança encontradas em sistema popular de 'casa inteligente'". Pesquisadores da Universidade de Michigan conseguiram invadir um sistema de casas inteligentes líder de mercado e obter o código PIN (*Personal Indentification Number*)[18] da porta de uma casa.

[16] SRLabs é um grupo de pesquisa de segurança que trabalha em consultoria e projetos internos, bem como ferramentas na vanguarda da pesquisa de segurança.

[17] Phishing é a tentativa fraudulenta de obter informações confidenciais como nomes de usuário, senhas e detalhes de cartão de crédito, por meio de disfarce de entidade confiável em uma comunicação eletrônica.

[18] O Número de Identificação Pessoal (PIN, sigla oriunda do original em inglês *Personal Identification Number*) é o número que antecedeu

Um software malicioso, como se fosse um lock-picking[19], foi utilizado em um dos ataques contra uma configuração experimental da linha de produtos SmartThings, da Samsung. Os pesquisadores não gostaram do que viram.

"*Pelo menos hoje, com a única plataforma de software IoT pública que examinamos, que existe há vários anos, existem vulnerabilidades de design significativas de uma perspectiva de segurança*" (Tradução nossa), disse Atul Prakash, professor de ciência da computação e engenharia da U-M. "Eu diria que não há problema em usar como hobby agora, mas não o usaria onde a segurança é fundamental."

Mesmo que dispositivos como cadeados, termostatos, fornos, lâmpadas e sensores de movimento, possam ser considerados seguros quando vistos individualmente, quando todos estão conectados e podem ser controlados remotamente, problemas de segurança vão surgir.

Os pesquisadores comprovaram o crescimento do uso dos produtos da linha SmartThings, o aplicativo Android[20] usado para gerenciar os dispositivos já havia sido baixado mais de 100.000 (cem mil) vezes. Além disso, quinhentos outros aplicativos, desenvolvidos por colaboradores, estavam disponíveis na plataforma da SamSung.

Durante as pesquisas, foi demonstrado que um dos aplicativos espionou a configuração de um PIN para uma fechadura inteligente e em seguida enviou o código via mensagem de texto para um potencial agente malicioso. O software de *lock-picking* estava disfarçado como um monitor para a bateria.

Também foi demonstrado que o alarme de incêndio poderia ser desativado por qualquer um dos aplicativos, apenas injetando mensagens falsas.

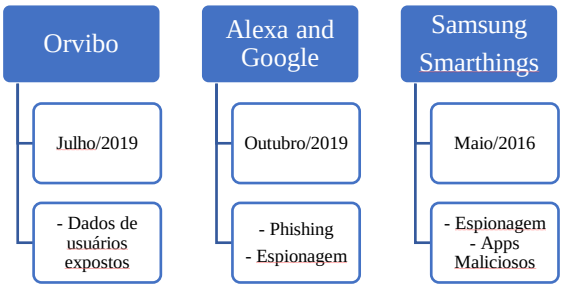
Mais de 40% (quarenta por cento) dos aplicativos verificados tinham mais funcionalidades que as especificadas em seus códigos. Além de problemas com autenticação e falhas na plataforma.

"*O ponto principal é que não é fácil proteger esses sistemas*" (Tradução nossa), disse Prakash. "*Existem várias camadas na pilha de software e encontramos vulnerabilidades entre elas, tornando as correções difíceis*." (Tradução nossa)

A Samsung disse que continuam a explorar "capacidades defensivas automatizadas de longo prazo para lidar com essas vulnerabilidades". Eles também estão analisando aplicativos antigos e novos em um esforço para garantir que a autenticação apropriada seja implementada, entre outras etapas.

A Figura 3 mostra um comparativo sobre falhas:

Figura 3: Comparativo entre as falhas citadas.



Fonte: Autor.

Será que essas falhas e vazamentos poderiam ser evitadas apenas com as Leis, frameworks e regulamentações já existentes?

as senhas nos bancos modernos, para acessar os caixas automáticos. (Wikipedia, 2020)

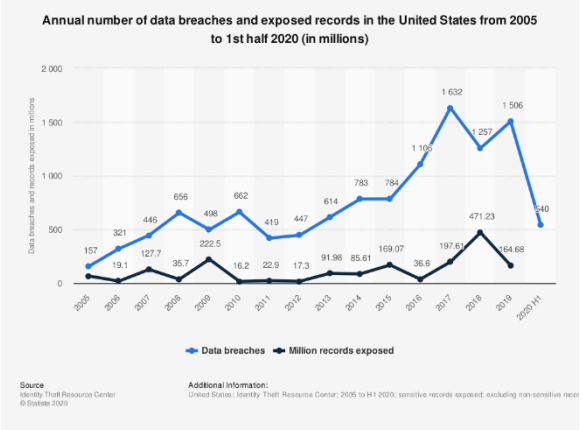
[19] O *lock-picking* é a prática de destravar uma fechadura manipulando os componentes do dispositivo de fechadura sem a chave original. (Wikipedia, 2020)

[20] Android é um sistema operacional (SO) baseado no núcleo Linux, desenvolvido por um consórcio de desenvolvedores conhecido como Open Handset Alliance, sendo o principal colaborador o Google. (Wikipedia, 2020)

A maioria delas sim. Se não totalmente evitadas, no mínimo teriam um impacto bem menor. No caso de dispositivos IoT, o NIST, através do *Cybersecurity for IoT Program*, sugere várias ações que, se aplicadas pelos fabricantes, poderiam pelo menos, reduzir as chances que as falhas ocorressem. Além de indicar essas práticas aos fabricantes; as publicações do NIST podem auxiliar os usuários e consumidores desses equipamentos a fazerem melhores escolhas, colocando à disposição conhecimento sobre práticas de ciber-segurança que, quando aplicadas, asseguram maior proteção a todas as informações transmitidas ou armazenadas nos dispositivos.

Como pode-se observar na Figura 4, o número de vazamento de dados e registros expostos tem aumentado rapidamente desde 2005.

Figura 4: Número de vazamentos de dados e quantidade de registros expostos desde 2005.



Fonte: Identity Theft Resource Center, 2020.

5. CONCLUSÃO

Como pode-se observar, as leis, melhores práticas e regulamentações em vigor, se seguidas, podem impactar muito positivamente a segurança da informação dos dispositivos e plataformas de IoT.

As leis e regulamentações, como a LGDP e a GDPR, são focadas no processamento e armazenamento dos dados pessoais, além dos direitos dos seus titulares.

Já os *frameworks*, como os do NIST, sugerem melhores práticas para serem aplicadas na indústria e organizações, além de servirem de apoio aos clientes e usuários, que saberão o que devem esperar desses produtos em termos de ciber-segurança.

No Brasil, não se tem uma entidade oficial similar ao braço de ciber-segurança do NIST – o NCCoE, onde suas publicações de requisitos mínimos e melhores práticas são fortemente adotadas por quem deseja gerenciar e reduzir os riscos de ciber-segurança nos produtos do ecossistema de IoT. Tem-se Associação Brasileira de Normas Técnicas (ABNT)[21], que por meio das normas da família ISO 27000[22], dispõe sobre a gestão da segurança da informação. Essas normas, tratam de requisitos e controles de segurança, gestão de riscos, governança e auditoria, entre outros. Essa família de normas é focada nas organizações em geral e em como devem gerir a segurança da informação. O problema com essas normas é que elas não são de fácil acesso, principalmente ao público em geral.

Algo como o NIST/NCCoE no Brasil, faria um trabalho similar ao do Instituto Nacional de Metrologia (Inmetro)[23], porém voltado para ciber-

[21] A ABNT é responsável pela elaboração das Normas Brasileiras (ABNT NBR), ela atua na avaliação da conformidade e dispõe de programas para certificação de produtos, sistemas e rotulagem ambiental. (ABNT, 2020)

[22] As normas da família ISO 27000 tratam da gestão da segurança da informação. (ABNT, 2002)

[23] O Instituto Nacional de Metrologia, Qualidade e Tecnologia - Inmetro - é uma autarquia

segurança. A princípio, traria orientações e melhores práticas para os fabricantes brasileiros e seus consumidores e adicionalmente cobraria e puniria fabricantes e desenvolvedores que não seguissem essas melhores práticas. De forma similar ao NIST, além dos requisitos mínimos de segurança para os equipamentos, as orientações deveriam tratar também da divulgação desses requisitos e guiar fabricantes e desenvolvedores sobre como comunicar as possíveis falhas aos seus clientes e usuários.

Como faz o Inmetro em suas áreas de atuação, essa entidade emitiria um selo, e para recebê-lo, os fabricantes teriam que seguir à risca as melhores práticas, que estipulariam um patamar mínimo de segurança para os dispositivos. As penalidades seriam aplicadas aos fabricantes e desenvolvedores que, caso não seguissem as melhores práticas, tivessem incidentes de segurança envolvendo seus produtos. A comunicação dos incidentes também é de suma importância, ela iria alertar os usuários dos dispositivos sobre as falhas, além de orientá-los sobre como mitigar o problema, seja com uma simples alteração de senha ou com atualizações de software fornecidas pelos fabricantes.

Atualmente, somente os criminosos que se aproveitam dessas falhas são punidos, mas fabricantes de desenvolvedores que não oferecem requisitos mínimos de segurança em seus produtos também deveriam ser responsabilizados.

No mundo da ciber-segurança é impossível se chegar ao ponto de se estar 100% seguro, por isso, se o fabricante ou desenvolvedor segue as leis e melhores práticas de segurança, não há por que eles serem punidos.

No Brasil tem-se ótimas leis para proteção de dados pessoais, como a LGPD e o Marco Civil da Internet, mas não se tem nada oficial no que diz respeito a *frameworks* voltados para ciber-segurança, em geral, usa-se bastante as normas da ABNT, mas não existe uma orientação geral do que deve ser seguido. Na Europa e nos Estados Unidos se têm ambos; estão bem mais avançados nesse aspecto. A Europa, como já foi dito, tem a GDPR, e tem a Lei sobre Ciber-segurança da União Europeia (*EU Cybersecurity Act*)[24], que atua de forma similar ao NIST. Os Estados Unidos têm, além de várias leis em vigor nos seus cinquenta estados, o Framework de Ciber-segurança (*Cybersecurity Framework*) e o Programa de Ciber-segurança para IoT (*IoT Cybersecurity Program*), ambos propostos pelo NIST.

No comparativo a seguir verifica-se que, comparado aos Estados Unidos e à Europa, uma adoção uniforme de um *framework* pode abrir portas para produtos brasileiros nesses dois mercados.

Tabela 1. Comparativo: Brasil, Europa e Estados Unidos.

	BRASIL	**Europa**	**Estados Unidos**
Proteção de Dados Pessoais	☑	☑	☑
Framework de Segurança	☒	☑	☑

Fonte: Autor.

federal, vinculada à Secretaria Especial de Produtividade, Emprego e Competitividade, do Ministério da Economia. Que tem como missão prover infraestrutura da qualidade para viabilizar soluções que adicionem confiança, qualidade e competitividade aos produtos e serviços disponibilizados pelas organizações brasileiras, em prol da prosperidade econômica e bem-estar da nossa sociedade. (Inmetro, 2018)

[24] A Lei sobre ciber-segurança da União Europeia renova e fortalece a Agência da UE para a ciber-segurança (ENISA) e estabelece um quadro de certificação de ciber-segurança em toda a UE para produtos, serviços e processos digitais.

Com ajustes nas leis em vigor, usando o que se tem de melhor mundo afora, como base e com a criação de algo similar ao braço de ciber-segurança do NIST, o Brasil estará mais bem posicionado no que se refere à ciber-segurança, não só para IoT mas para toda as áreas da Tecnologia da Informação. Os profissionais e entidades ligadas a Engenharia precisam colaborar para que no futuro o Brasil conquiste uma grande fatia dos investimentos que estão previstos para o mercado da Internet das Coisas.

Ainda, podem-se observar, no Brasil inciativas mais abrangentes, como as do Projeto Estratégico de Defesa Cibernética, especialmente com a criação do Centro de Defesa Cibernética (CDCiber), em 2010. As premissas de trabalho desse órgão são coordenar e integrar esforços dos vetores de Defesa Cibernética. De acordo com o portal do EPEx – Escritório de Projetos do Exército Brasileiro -, um enfoque especial foi destinado ao desenvolvimento de doutrina de proteção dos próprios ativos, bem como a capacidade de atuar em rede, na de implementar pesquisa científica voltada ao tema de segurança cibernética e na indução de capacidade tecnológica nacional. (EPEx, 2017)

O CDCiber é um ótimo exemplo da capacidade para desenvolvimento ou adequação de *framework*, com melhores práticas e requisitos mínimos de segurança que contemplem a indústria e fornecedores de dispositivos e soluções de IoT para o mercado Brasileiro.

AGRADECIMENTOS

Agradeço a **Deus**, por todo conforto espiritual que me foi concedido, durante todos os obstáculos vencidos nessa jornada.

Agradeço ao meu orientador, **Professor Javier**, por aceitar conduzir o meu trabalho de pesquisa.

A todos os meus professores do curso de **Engenharia da Computação** do **UniCEUB** pela excelência da qualidade técnica de cada um.

Aos meus pais **Sinair** e **Márcia** que sempre estiveram ao meu lado me apoiando ao longo de toda a minha trajetória.

À minha maravilhosa esposa **Mariana** e à querida filha **Alice**, pela compreensão, paciência e apoio demonstrado durante o período do projeto.

Referências

About Orvibo. Orvibo, 2018. Disponível em: < https://www.orvibo.com/en/about/about_us.html>. Acesso em 16 de Novembro de 2020.

Android. Wikipedia, 2020. Disponível em: <https://pt.wikipedia.org/wiki/Android>. Acesso em 18 de Novembro de 2020.

Annual number of data breaches and exposed records in the United States from 2005 to 1st half 2020. Statista, 2020. Disponível em: < https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>. Acesso em 02 de Dezembro de 2020.

ARBOR, Ann. Hacking into homes: 'Smart home' security flaws found in popular system. Michigan News, 2016. Disponível em: < https://news.umich.edu/hacking-into-homes-smart-home-security-

flaws-found-in-popular-system/>. Acesso em 18 de Novembro de 2020.

ATOUI, Roland. IoT and GDPR: Challenges and Opportunities. IoT for All, 2019. Disponível em: <https://www.iotforall.com/iot-gdpr-opportunity-privacy-by-design>. Acesso em 17 de Novembro de 2020.

CIMPANU, Catalin. Alexa and Google Home devices leveraged to phish and eavesdrop on users, again. ZDNet, 2019. Disponível em: <https://www.zdnet.com/article/alexa-and-google-home-devices-leveraged-to-phish-and-eavesdrop-on-users-again>. Acesso em 09 de Novembro de 2020.

Conheça a ABNT. ABNT, 2020. Disponível em: <http://www.abnt.org.br/abnt/conheca-a-abnt>. Acesso em 20 de Novembro de 2020.

DE OLIVEIRA, Nairobi; GOMES, Moisés; LOPES, Ronaldo; NOBRE, Jeferson. Segurança da Informação para Internet das Coisas (IoT): Uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD). Curso Superior de Tecnologia em Segurança da Informação. Universidade do Vale do Rio dos Sinos. Rio Grande do Sul, 2018.

FAGAN, Michael; MEGAS, Katerina; SCARFONE, Karen; SMITH, Matthew. Foundational Cybersecurity Activities for IoT Device Manufacturers. NIST. Maio, 2020. Disponível em: < https://doi.org/10.6028/NIST.IR.8259>. Acesso em 16 de Novembro de 2020.

FAGAN, Michael; MEGAS, Katerina; SCARFONE, Karen; SMITH, Matthew. IoT Device Cybersecurity Capability Core Baseline. NIST. Maio, 2020. Disponível em: < https://doi.org/10.6028/NIST.IR.8259A>. Acesso em 16 de Novembro de 2020.

GDPR - General Data Protection Regulation. Página Inicial. Disponível em:<https://gdpr-info.eu>. Acesso em: 20 de Outubro de 2020.

GYARMATHY, Kaylie. Comprehensive Guide to IoT – Statistics you need to know in 2020. VXCHNGE, 2020. Disponível em: < https://www.vxchnge.com/blog/iot-statistics>. Acesso em: 20 de Outubro de 2020.

Inmetro. Página Institucional. Inmetro, 2018. Disponível em: < https://www4.inmetro.gov.br/acesso-a-informacao/institucional>. Acesso em: 20 de Novembro de 2020.

Kevin Ashton – Entrevista exclusiva com o criador do termo "Internet das Coisas", FINEP, 2015. Disponível em: <http://finep.gov.br/noticias/todas-noticias/4446-kevin-ashton-entrevista-exclusiva-com-o-criador-do-termo-internet-das-coisas>. Acesso em: 20 de Outubro de 2020.

Kevin Ashton. Wikipedia, 2020. Disponível em: <https://en.wikipedia.org/wiki/Kevin_Ashton>. Acesso em: 20 de Outubro de 2020.

KITCHIN, Rob; DODGE, Martin. The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation and Prevention. Journal of Urban Technology. Dezembro, 2017. Disponível em: < https://doi.org/10.1080/10630732.2017.1408002>. Acesso em 16 de Novembro de 2020.

LGPD – Lei Geral de Proteção de Dados Pessoais, 2018. Página Inicial. Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Acesso em: 20 de Outubro de 2020.

National Cybersecurity Center of Excellence (NCCoE), 2012. About the Center. Disponível em: < https://www.nccoe.nist.gov/about-the-center>. Acesso em: 16 de Novembro de 2020.

NIST - National Institute of Standards and Technology. Página Inicial. Disponível em: <https://www.nist.gov>. Acesso em: 20 de Outubro de 2020.

Normativos e Frameworks de Segurança Cibernética: Leis, Normas, Controle e Gestão de Riscos de Segurança de Informação. Governo do Brasil, 2019. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/normativos-e-frameworks-de-seguranca-cibernetica>. Acesso em 20 de Novembro de 2020.

Número de identificação pessoal. Wikipedia, 2020. Disponível em: < https://pt.wikipedia.org/wiki/Número_de_identificação_pessoal>. Acesso em 18 de Novembro de 2020.

PATEL, Rushabh. IoT and home automation: What does the future hold? IoT Now, 2020. Disponível em: <https://www.iot-now.com/2020/06/10/98753-iot-home-automation-future-holds>. Acesso em 16 de Novembro de 2020.

RansomWare. Wikipedia, 2020. Disponível em: < https://pt.wikipedia.org/wiki/Ransomware>. Acesso em 16 de Novembro de 2020.

Smart Home Technology. Wikipedia, 2020. Disponível em: < https://en.wikipedia.org/wiki/Smart_home_technology>. Acesso em 09 de Novembro de 2020.

TEICHER, Jordan. The Little-known story of the first IoT device. IBM, 2018. Disponível em: < https://www.ibm.com/blogs/industries/little-known-story-first-iot-device>. Acesso em: 20 de Outubro de 2020.

TELES, Guilherme. O que é o NIST CyberSecurity Framework? Janeiro, 2020. Disponível em: < https://guilhermeteles.com.br/o-que-e-o-nist-cybersecurity-framework/>. Acesso em 20 de Novembro de 2020.

The EU Cybersecurity Act. European Comission. Fevereiro, 2020. Disponível em: < https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act>. Acesso em; 20 de Novembro de 2020.

What is a smart city? Cisco Systems Inc., 2020. Disponível em: <https://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities/what-is-a-smart-city.html>. Acesso em 09 de Novembro de 2020.

What is the Internet of Things (IoT) and how can we secure it? NIST Cybersecurity for IoT Program, 2016. Disponível em: <https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program>. Acesso: 20 de Outubro de 2020.

WINDER, Davey. Confirmed: 2 Billion Records Exposed in Massive Smart Home Device Breach. Forbes, 2019. Disponível em: < https://www.forbes.com/sites/daveywinder/2019/07/02/confirmed-2-billion-records-exposed-in-massive-smart-home-device-

breach/amp>. Acesso em 09 de Novembro de 2020.

WOLFORD, Ben. What is GDPR, the EU's new data protection law? GDPR, 2018. Disponível em: < https://gdpr.eu/what-is-gdpr>. Acesso em 16 de Novembro de 2020.

Programa de Defesa Cibernética. EPEx, 2017. Disponível em: < http://www.epex.eb.mil.br/index.php/defesa-cibernetica>. Acesso em: 02 de Dezembro de 2020.