CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA
CURSO DE GRADUAÇÃO TECNÓLOGO EM REDES DE COMPUTADORES

DIEGO SOARES PEREIRA
ITALO CAVALCANTI
RAMON PINTO LINS

SEGURANÇA DE DADOS E IOT:
A IMPORTÂNCIA DA SEGURANÇA DE DADOS E IOT

RECIFE/2023

DIEGO SOARES PEREIRA
ITALO CAVALCANTI
RAMON PINTO LINS

SEGURANÇA DE DADOS E IOT:
A IMPORTÂNCIA DA SEGURANÇA DE DADOS E IOT

Trabalho Conclusão de Curso apresentado ao Centro Universitário Brasileiro - UNIBRA, como requisito parcial para obtenção do título de ecnólogo em Redes de Computadores.
Professor Orientador: Ameliara Freire Santos de Miranda

RECIFE/2023

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 2338/ O.

P436s Pereira, Diego Soares.

Segurança de dados e IoT: a importância da segurança de dados e IoT / Diego Soares Pereira; Italo Cavalcanti; Ramon Pinto Lins. - Recife: O Autor, 2023.

26 p.

Orientador(a): MSc. Ameliara Freire Santos de Miranda.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – UNIBRA. Tecnólogo em Redes de Computadores, 2023.

Inclui Referências.

1. Internet. 2. Segurança da informação. 3. IoT. I. Cavalcanti, Italo. II. Lins, Ramon Pinto. III. Centro Universitário Brasileiro. - UNIBRA. IV. Título.

CDU: 004

Dedicamos esse trabalho aos nossos pais.

AGRADECIMENTOS

Dedicamos este trabalho primeiramente a Deus, por ser essencial em nossas vidas, aos os nossos professores e familiares. A experiência de uma produção compartilhada na comunhão com amigos nesses espaços foram as melhores experiências de nossa formação acadêmica.

“A imaginação é mais importante que o conhecimento, porque o conhecimento é limitado, ao passo que a imaginação abrange o mundo inteiro.”
(Albert Einstei

SUMÁRIO

Resumo: O objetivo do estudo é identificar a importância do uso da tecnologia IoT (Internet das coisas) com segurança em seus dados. Essencialmente, um ecossistema de IoT (Internet das coisas) consiste em dispositivos inteligentes que usam processadores, sensores e *hardware* de comunicação integrados para coletar, enviar e processar dados adquiridos de seu ambiente. A justificativa e relevância para este estudo está na necessidade de compreender que a Internet das Coisas trará mudanças significativas na gestão e operação de empresas e organizações. Mas para o sucesso do seu funcionamento, necessita de segurança em seus dados. Em que ponto o funcionamento das IoTs fornece segurança de dados aos seus usuários? O estudo é uma revisão bibliográfica. A Internet das Coisas é uma das tecnologias mais difundidas desse tempo. A penetração da Internet e o uso de redes na vida cotidiana tornou-se parte integrante dela, pois as áreas em que é aplicada dizem respeito à totalidade das atividades da pessoa média no mundo ocidental. Mas à medida que encontram aplicações em áreas como saúde, transporte, energia, comércio, cidades inteligentes e casas inteligentes, a questão da segurança é mais relevante do que nunca.

Palavras-chave: *Internet*. Segurança da informação. Iot.

1. INTRODUÇÃO

A Internet das Coisas (IoT) é uma tecnologia em crescimento que está cada vez mais entrando na vida das pessoas. A ideia básica da IoT é integrar dispositivos em objetos/aparelhos do cotidiano para torná-los inteligentes. Esses dispositivos requerem a capacidade de coletar, processar e transmitir informações. Isso só é possível por meio do uso e integração de tecnologias existentes, como redes de sensores sem fio (WSN), identificação por radiofrequência (RFID) e tecnologia NFC.

Essencialmente, um ecossistema de IoT (Internet das coisas) consiste em dispositivos inteligentes que usam processadores, sensores e *hardware* de comunicação integrados para coletar, enviar e processar dados adquiridos de seu ambiente. Os dispositivos IoT compartilham os dados do sensor que coletam conectando-se a um *gateway* IoT ou outro dispositivo, onde os dados são enviados para a nuvem para serem analisados ou verificados localmente.

Às vezes, esses dispositivos se comunicam com outros dispositivos relacionados e agem de acordo com as informações que recebem uns dos outros. Os dispositivos executam a maior parte do trabalho sem intervenção humana, embora as pessoas possam interagir com os dispositivos.

A justificativa e relevância para este estudo está na necessidade de compreender que a *Internet* das Coisas trará mudanças significativas na gestão e operação de empresas e organizações. Mas para o sucesso do seu funcionamento, necessita de segurança em seus dados. Os dados coletados podem ser usados para melhorar o desempenho, identificar e prever as necessidades de pessoas e organizações antes que elas surjam.

Dentro deste contexto, surge uma problemática para ser resolvida: Em que ponto o funcionamento das IoTs fornece segurança de dados aos seus usuários? A IoT não seria possível sem sensores para detectar ou medir qualquer alteração no ambiente, para produzir dados que possam relatar seu *status*, ou mesmo interagir com o ambiente. As tecnologias de detecção permitem que os dispositivos conheçam verdadeiramente o mundo físico e suas pessoas.

O objetivo do estudo é identificar a importância do uso da tecnologia IoT com segurança de dados. E tem como objetivos específicos: Apresentar conceitos e contextos na área de segurança e tecnologia IoT; identificar as leis de crime e

segurança cibernética no Brasil e no mundo; e compreender as falhas e as possíveis soluções na segurança da IoT.

O estudo é uma revisão bibliográfica, com características descritivas e qualitativas. Pesquisas do tipo têm o objetivo primordial à exposição dos atributos de determinado fenômeno ou afirmação de relações entre as variáveis (GIL, 2008). Assim, recomenda-se que apresente atributos do tipo: analisar a atmosfera como fonte direta dos dados e o pesquisador como um instrumento interruptor; não agenciar o uso de artifícios e métodos estatísticos; tendo como apreensão maior a interpretação de fenômenos e a imputação de resultados; o método deve ser o foco principal para a abordagem e não o resultado ou o fruto; a apreciação dos dados deve ser atingida de forma intuitiva e indutivamente através do pesquisador (GIL, 2008).

Várias bibliografias de autores com expressão significativa em campo científico foram pesquisadas, oportunidade que trouxe as principais ideias adicionadas, tendo como alvo fundamentar a proposta deste trabalho. O levantamento dos dados e das informações relevantes para a investigação e o entendimento das questões propostas, utilizando técnicas de bibliografia indireta. Também foram pesquisadas e coletadas informações relevantes e atualizadas na Internet, acerca do tema, delineando a reflexão conforme se veem, bem como as referências bibliográficas citadas neste estudo.

2 REFERENCIAL TEÓRICO

IoT (Internet das coisas) é um novo modelo de conectar objetos do mundo real em um sistema único cujos elementos são capazes de se comunicar uns com os outros (BORGIA, 2014). A ideia básica deste modelo é a existência de vários dispositivos (*tags*, sensores, telefones celulares, etc.) que podem trocar informações através de uma rede sem fio, a fim de alcançar objetivos mútuos. O termo Internet das Coisas foi introduzido pela primeira vez por Kevin Ashton em 1999, quando ele estava pesquisando novas possibilidades de aplicação da tecnologia RFID e da Internet na cadeia de fornecimento da *Procter & Gamble* (BORGIA, 2014). Assim, Borgia complementa que:

> A maioria dos dados disponíveis na Internet foi criada por seres humanos, inserindo dados manualmente, pressionando um botão de gravação ou digitalizando um código de barras. O problema básico é que as pessoas têm tempo, atenção e precisão limitados, o que significa que eles não são bons o suficiente para adquirir dados sobre as coisas no mundo real (BORGIA, 2014, p.49).

Se os computadores tivessem todos os dados e informações sobre coisas, adquiridos sem a ajuda de pessoas; perdas e custos seriam significativamente reduzidos, o planejamento, a tomada de decisões e os processos de controle melhorados (BORGIA, 2014).

A Internet das Coisas (IoT) é uma tecnologia de computação que permite que dispositivos físicos troquem dados entre si. Os dispositivos físicos podem ser objetos, animais e máquinas digitais, dados os identificadores especiais e a capacidade de trocar informações pela Internet sem intervenção humana (TIMM, 2006).

O uso disso na logística moderna está ganhando espaço, com os desenvolvedores de *softwares* trabalhando sem parar para enfrentar desafios importantes. Por outro lado, a nuvem (ou, mais formalmente, a computação em nuvem) é a capacidade de acessar dados pessoais ou comerciais usando a Internet, em vez do disco rígido físico do computador. Acredita-se que Internet das Coisas terá um enorme impacto no rastreamento e rastreio de mercadorias enquanto estão sendo transportadas do fabricante para o consumidor final. Pode ser descrita como objetos físicos que foram conectados à internet de alguma forma (FLOERKEMEIER; LAMPE; RODUNER, 2007).

Considera-se que a Internet das Coisas pode ter um alto impacto em todos os aspectos da vida cotidiana. Prevê-se a integração do mundo físico no mundo digital ou vice-versa (TIMM, 2006). Empresas e países já avaliaram a importância da IoT e começaram a se mover em posições estrategicamente vantajosas para explorar o máximo valor da IoT. Por exemplo, Oliveira (2013) considera a IoT uma das cinco tecnologias civis disruptivas, que tem um impacto potencialmente importante sobre os interesses do país na economia até 2025. Oliveira (2013) aconselha as empresas a iniciar ou continuar concentrando-se em aumentar seus processos e modelos de negócios com soluções de IoT e obter conhecimento especializado o mais rápido possível.

Gartner (2016) também especula que, até 2025, a maioria dos novos processos de negócios será apoiada por tecnologias e soluções de IoT de uma forma ou de outra. Ao mesmo tempo, Gartner (2016) prevê que até 2025 mais de 20 bilhões de dispositivos estejam conectados à Internet. Em uma nota à parte, o autor também assume que neste mesmo prazo haverá um mercado indevido no valor de US $5 bilhões para dados falsos de sensores, o que enfatiza a necessidade de reputação da informação e técnicas de avaliação em IoT.

Seguindo esse raciocínio, para que a IoT tenha sucesso, um ambiente de confiança deve ser estabelecido e destacado novamente, a IoT pode muito bem ser considerada uma tecnologia sensacionalista (FENN; LEHONG, 2015). Como a IoT é um conceito relativamente novo e sob alta cobertura de mídia, empresas e pesquisadores, não é de surpreender que o termo em si e o campo de pesquisa relacionado, não tenham por hora uma definição comumente aceita e estabelecida.

As ideias centrais comumente mencionadas da IoT são a integração contínua de objetos virtuais e físicos em uma rede, sua interação contextual e cooperação para alcançar objetivos comuns e sua presença onipresente no mundo real e digital (MAZHELIS *et al*., 2013).

A primeira ideia que levou ao conceito atual de IoT foi o objetivo de integrar as coisas físicas nos sistemas digitais. O desenvolvimento foi impulsionado pela ideia de melhorar o controle, seja nas cadeias de suprimento, no comércio e no gerenciamento de estoque, aplicando Códigos Eletrônicos de Produto (EPC) a produtos e itens. Esses EPCs podem ser usados para armazenar e compartilhar informações sobre os itens e produtos aos quais estão vinculados.

A informação é compartilhada usando interfaces padronizadas e utiliza identificação por radiofrequência (RFID), bem como a Internet e sistemas de comunicação relacionados. Pesquisas e esforços iniciais em matéria de padronização foram realizados, visando introduzir uma arquitetura global padronizada para EPC, e pelo *Auto-ID Labs*, que se concentra em pesquisas sobre redes RFID e sensores emergentes e técnicas (MAZHELIS *et al*. 2013).

Objetos ou Coisas equipadas com etiquetas RFID, geralmente consistindo de uma antena e uma informação de armazenamento de microchip, podem ser rastreadas por leitores RFID que podem, portanto, ler as informações armazenadas nas etiquetas RFID. Assim, sistemas de computador podem obter informações verdadeiras, isto é, de objetos físicos. O termo Internet das Coisas é atribuído aos *Auto-ID Labs* (Fenn; Lehong, 2015) e mais tarde foi formalmente definido pela União Internacional de Telecomunicações (2005).

No entanto, Atzori *et al*. (2010) também dizem que a IoT pode e não será meramente um sistema EPC global baseado em RFID. Mais itens diferentes e tipos de coisas serão adicionados e conectados usando diferentes tecnologias de comunicação (por exemplo, NFC, *Bluetooth Low Energy* (BLE), etc.).

Entende-se que as coisas precisam ser gerenciadas e organizadas em redes (por exemplo, *Wireless Sensing and Actuating Networks* (WSAN)). A próxima heterogeneidade já foi considerada na definição formal de IoT fornecida pela União Internacional de Telecomunicações (2005). A definição afirma que a Internet não só pode conectar qualquer pessoa em qualquer momento e em qualquer lugar, mas qualquer coisa a qualquer hora e em qualquer lugar.

Essa visão se concentra mais no aspecto de rede da IoT e Atzori *et al.* (2010) o nomeiam Visão de Internet da IoT. Tendo concordado com essas ideias e com a IoT ganhando um interesse significativo, tanto a pesquisa quanto a indústria tentaram desenvolver casos de uso relevantes para a IoT. Entre outros, casos de uso vantajosos na gestão da cadeia de suprimentos, logística e gestão de estoques foram identificados (ATZORI *et al*., 2010).

Além disso, a geladeira inteligente apresentada pela LG no ano 2000 é usada como um exemplo proeminente de IoT para os consumidores (ROTHENSEE, 2008). Com custos decrescentes e aumento da disponibilidade de tecnologias IoT relevantes (por exemplo, etiquetas RFID, sensores de baixa energia e BLE, etc.), o número de coisas conectados à Internet aumentou e rapidamente superou o número

de dispositivos endereçáveis usados pelo atual esquema de endereçamento da Internet (IPv4).

Com a introdução do IPv6 para acomodar um número praticamente inesgotável de dispositivos endereçáveis em 2011 e a introdução da Internet das coisas para *Gartner's Hype Cycle* de Tecnologias Emergentes no mesmo ano, o conceito de Internet das Coisas finalmente se tornou visível para o público em geral (MADAKAM *et al.* 2015).

Com um vasto número de coisas conectadas, questões relacionadas à busca, organização e armazenamento de informações tornaram-se aparentes. Como já foi observado, a IoT implica inevitavelmente um certo grau de heterogeneidade. Portanto, os meios tradicionais de gerenciar e pesquisar informações tornam-se impraticáveis neste contexto (ATZORI *et al*. 2010).

As tecnologias semânticas (por exemplo, *Resource Description Framework* (RDF), *Web Ontology Language* (OWL), etc.) são consideradas uma solução potencial para esses desafios. É por isso que surgiu a Visão Orientada por Semântica da IoT (ATZORI *et al*. 2010).

Para o cenário atual da IoT, ela carece de uma definição comumente aceita e estabelecida devido à alta cobertura e interesse da mídia de todos os diferentes domínios, bem como à novidade do domínio de pesquisa. Cada um desses domínios ou grupos de interesse, que se concentram em diferentes aspectos das ideias centrais e entram em diferentes estágios da “ascensão da IoT”, pode ser vagamente atribuído a uma das perspectivas da IoT mencionadas (ATZORI *et al*. 2010). Essas perspectivas são orientadas a coisas, orientadas à *Internet* e Perspectiva Semântica da IoT.

2.1 SEGURANÇA DE DADOS OU INFORMAÇÕES

As nações de países emergentes, como a China, a Índia e a Indonésia, publicaram seus regulamentos de segurança de dados ou informações recentemente, enquanto países desenvolvidos como os Estados Unidos e a Alemanha têm regulamentado há mais de uma década (COSTA, 2014). Outros países, como o Brasil, ainda se esforçam para concordar com uma regulamentação apropriada. De acordo com Costa (2014) os padrões da indústria também estão sendo úteis em "regulamentar a segurança", particularmente nas nações em que

faltam regras de segurança de dados, mas também em todas as nações, onde a regulamentação pode ser desconhecida ou inconsistente.

2.1.1 Preocupação de títulos

Dez em dez empresários ou executivos afirmaram prontamente que reconhecem a importância da segurança e proteção de dados, mas nem todos adotam planos para a preservação da confidencialidade, disponibilidade e integridade desses dados ou a implementação de controles para manter a continuidade do negócio, o que garantirá sua disponibilidade e a manutenção das atividades comerciais quando houver problemas (DOURADO, 2013).

Esta situação insustentável, representada pelo conhecimento da importância da informação, ao mesmo tempo que não atribui recursos suficientes para sua preservação, é extremamente relevante e justifica a investigação. Desde a antiguidade, o homem tentou controlar essas informações que ele julga serem importantes. Na China antiga, a própria língua escrita serviu como um tipo de código secreto, porque apenas as classes superiores podiam aprender a ler e escrever. Povos como os egípcios e os romanos também deixaram um registro histórico de sua preocupação com o tratamento de certas informações, especialmente com valor estratégico e comercial (DOURADO, 2013).

Verifica-se que, hoje em dia, muitas organizações dedicam grande parte de sua atenção a ativos físicos e financeiros tangíveis, mas pouco aos recursos informativos que também constatam que a informação assumiu uma importância fundamental na realização de negócios, uma vez que isso se tornou cada vez mais dinâmico e globalizado. Dourado (2013) argumenta que essa falta de preocupação e preparação de muitos executivos e empresários que operam pequenas empresas pode resultar em perdas materiais, bem como perda social considerável quando informações críticas sobre clientes são divulgadas.

2.2 A EVOLUÇÃO DA TECNOLOGIA E SUAS MUDANÇAS

A evolução da tecnologia da informação (Laudon *et al*., 2014) provocou mudanças no comportamento social, ao mesmo tempo em que aumentou os problemas éticos envolvendo crime, privacidade, individualidade, empregos, saúde e

condições de trabalho. De acordo com Schneier (2007), o conceito de crime informático inclui as seguintes categorias:

- Uso não autorizado, acesso, modificação e destruição de *hardware*, *software*, dados ou recursos de rede;
- Liberação não autorizada de informações;
- Cópias de *software* não autorizadas; e
- Negação de acesso ao próprio *software* de *hardware*, dados ou recursos de rede.

A preocupação constante com a segurança da informação existe em todos os setores, desde os bancos de dados das empresas de cartão de crédito até aqueles que fornecem uma variedade de serviços. As violações da segurança ocorrem com uma frequência cada vez maior, e envolvem metas e razões cada vez mais variadas, incluindo *hackers* que buscam lucros pessoais, usuários com intenções criminosas e até mesmo empresas envolvidas na espionagem industrial (RAYMOND *et al*., 2004).

Nem as entidades que estão bem preparadas em relação à segurança da informação estão totalmente livres de tais problemas. Uma revista brasileira especializada em segurança da informação (REVISÃO DE SEGURANÇA, 2013) traz a conta de um ataque ao Corpo de Marines dos EUA, que levou à divulgação de dados confidenciais de cerca de cem mil funcionários, esta informação foi disponibilizada por mais de seis meses em um *site* da Internet.

2.2.1 Práticas de segurança

Os processadores de dados no Brasil são necessários e esperam seguir medidas razoáveis, tanto técnicas como físicas, para proteger a segurança de dados pessoais (PEIXOTO, 2010). No entanto, atualmente não há requisitos específicos ou diretrizes sobre como essas medidas de segurança devem ser implementadas. De acordo com Peixoto (2010) a lei jurisprudencial exige que os provedores de serviços mantenham registros de acesso, como endereços IP e informações de *login* por um período de tempo razoável para ajudar a identificar usuários que possam ter cometido crimes. Além disso, os proprietários de dados ou dispositivos violados não são obrigados a notificar as autoridades públicas.

2.2.2 Execução

Atualmente, não há agências no Brasil que imponham os regulamentos de proteção de dados, no entanto, a aprovação da Lei 12.735 em 2012 é um primeiro histórico para o Brasil no que diz respeito ao combate e execução do Crime Cibernético (PEIXOTO, 2010). Embora existam agências que garantem a proteção de dados, processos civis ou ações coletivas podem ser criados pelas autoridades públicas ou pela pessoa em questão. Jansen, Hinzpeter e Schwarzbart (2013) relatam que multas administrativas podem ser estabelecidas em montantes até US$ 1,5 milhão de dólares. Os prêmios de dano podem atingir aproximadamente US$ 7.500 por ações individuais ou mais de US$ 1 milhão por ação coletiva.

2.3 FRAUDE VIRTUAL

Os casos de fraude virtual (REVISÃO DE SEGURANÇA, 2013), que incluem ataques que resultam na negação de serviços, bem como redes Zumbi, vírus, *worms*, *spyware*, roubo de identidade, engenharia social e invasões, são estimados como danos no valor de US $ 67,2 bilhões em 2005 nos Estados Unidos. No Brasil, de acordo com as investigações da Equipe Brasileira de Resposta a Emergências de Computadores, as tentativas de fraude virtual registrada em 2005 mostraram um aumento de 579% em relação ao ano anterior, com 68 mil incidentes; embora cerca de 40% destes não tiveram êxito. Cerca de duas mil empresas foram investigadas; 1.300 destas (64%) registraram incidentes envolvendo segurança da informação em 2005 (REVISÃO DE SEGURANÇA, 2013).

2.3.1 Leis de *Cibercrimes* 12.735 e 12.737 (2012)

As duas primeiras leis da *cibercriminalidade* na história brasileira, 12.735 e 12.737 foram assinadas em 30 de novembro de 2012 (BKBG, 2013). A Lei 12.735 obriga as agências de aplicação da lei a designar unidades especiais para combater o *cibercrime*. De acordo com Costa (2014) a Lei 12.737 declara o ato de intrusões de computador com a intenção de alterar, coletar ou destruir informações como um crime se o intruso não recebeu autorização do proprietário dos computadores e se o intruso violar um mecanismo de segurança. Ele criminaliza ainda mais qualquer

"instalação de vulnerabilidades" não autorizadas. A Lei 12.737 também diz sobre distribuir, vender ou produzir programas de computador que tenham esse objetivo de invasão ilegal.

O projeto de lei foi redigido em 2009 e foi apresentado como uma peça de legislação colaborativa de cooperação. Milhares de pessoas já participaram de consultas públicas *online* para ajudar a moldar a direção da conta. O Comitê Diretor de Internet no Brasil (2016) informa que esta é atualmente a principal iniciativa de regulação da Internet, neutralidade da rede, privacidade, governança da Internet e comércio eletrônico, entre outras coisas. O projeto de lei é relevante para a proteção de dados através de três aspectos: riscos de vazamento de dados, processamento de dados sensíveis e publicidade comportamental. É uma maneira de segmentarem anúncios aos usuários com base em seus hábitos e interesses.

Um grande desafio com o registro de quantidades consideráveis de informações é a possibilidade de os dados serem "vazados" ou serem divulgados acidentalmente. Sem uma política de gestão adequada para tal informação, o descuido pode levar à divulgação pública involuntária ou mesmo premeditada. Os episódios de dados vazados tornaram-se frequentes no Brasil, e a indignação pública exigiu uma legislação para combater isso. O projeto de lei aborda este problema, exigindo que estes tipos de dados sejam tratados de forma a minimizar a possibilidade de acesso não autorizado (COSTA, 2014).

Aqueles que processam os dados são ainda obrigados a utilizar as medidas técnicas e administrativas adequadas ao nível de tecnologia, aos dados específicos e ao tipo de processamento, para evitar desígnios intencionais para divulgação internacional ou acesso não autorizado a informações pessoais. O *Draft Bill* considera o processamento de dados pessoais como uma atividade de risco e declara que, se houver uma ocorrência de dados pessoais vazados ou outros danos à propriedade, aquele que processa diretamente os dados será responsável (COSTA, 2014).

O processamento de dados sensíveis é outro tema de preocupação discutido no projeto de lei. É definido na conta como qualquer informação pessoal em que a natureza por si só pode resultar em prejuízo para o proprietário. E nomeiam ainda exemplos de dados sensíveis para incluir informações étnicas / raciais, crenças religiosas, filosóficas ou morais, preferências sexuais e informações pessoais sobre saúde, genética e biometria (REVISÃO DE SEGURANÇA, 2013).

O *Draft Bill* (MCI) proíbe a divulgação obrigatória de tais dados, e também proíbe a criação de um banco de dados que revele, direta ou indiretamente, dados confidenciais, exceto quando permitido por disposição legal expressa. Ele afirma ainda que a retenção de dados sensíveis é aceitável, com o consentimento do proprietário. Os dados sensíveis também podem ser mantidos por pessoas apropriadas quando necessário para o cumprimento da regulamentação, ou está dentro do escopo da pesquisa, ou se a informação foi previamente divulgada pelo seu proprietário. Finalmente, afirma que o uso de dados confidenciais para discriminar seu proprietário é proibido (COSTA, 2014).

2.4 POSIÇÃO DE SEGURANÇA DA INFORMAÇÃO NO BRASIL

Em pesquisa recente, o Comitê de Gerenciamento para Uso da Internet no Brasil (REVISÃO DE SEGURANÇA, 2013) verificou uma migração do alvo de ataques das grandes empresas para indivíduos e empresas menores, em grande parte devido à falta de segurança em relação ao acesso à Internet. Vários fatores contribuíram para essa migração, incluindo o fato de haver um aumento no número de usuários residenciais e um aumento correspondente no tempo gasto na navegação na *web*, com a consequente exposição ao ataque, muitos desses usuários residenciais e pequenos empresários não estão especialmente preocupados com a segurança da Internet e limitam sua proteção a um *software* antivírus simples.

Além disso, atacar grandes servidores corporativos tornou-se mais difícil, especialmente com investimentos em *software* de proteção, como *firewalls* e sistemas de detecção de intrusão. Isso significa que se tornou relativamente mais fácil e eficiente atacar diretamente os usuários residenciais e de pequenas empresas, enquanto que os ataques aos servidores corporativos representam uma porcentagem menor. Tais ataques tendem a envolver o uso da técnica de engenharia social, que envolve o contato do usuário de alguma forma e enganá-lo para revelar informações confidenciais ou, de alguma forma, explorar sua confiança. Isso leva à sabotagem do computador do usuário através da introdução de vários tipos de programas, incluindo vírus, cavalos de troia e *worms* (PEIXOTO, 2010).

Os vírus e os cavalos de troia são os mais comuns, representando 50,34% e 31,13% dos ataques, respectivamente. *Worms* são as invenções mais recentes. Eles

são programas de auto repetição semelhantes a um vírus, exceto que um vírus infecta um programa e precisa que esse programa hospedeiro se propague, considerando que um vírus é um programa completo por si só e não exige outro programa de propagação e a infecção do setor de inicialização. Mesmo que os vírus não se reproduzam, eles podem ser transmitidos por meio de *e-mail*. Uma vez que um *worm* está instalado, a máquina pode ser controlada remotamente, e o invasor pode utilizá-lo para atividades tão nefastas como o envio de *Spam* ou o bloqueio de *sites*.

Estes mecanismos muitas vezes levam à perda de configuração do sistema (11,2%) e tentativas não autorizadas de acesso (10,89%). De acordo com (Dourado, 2013), a melhoria da segurança depende de uma variedade de ações, especialmente a educação dos usuários sobre as ameaças e formas de proteção disponíveis. Das empresas investigadas, 19,69% tinham um programa de treinamento voltado para a segurança da informação, e para aqueles com mais de 500 funcionários, isso aumentou para mais de 40%.

2.5 EMPRESAS BRASILEIRAS EM RELAÇÃO À SEGURANÇA DA INFORMAÇÃO

A segurança da informação é submetida a tratamento diferenciado, dependendo da cultura local. As preocupações específicas sobre a proteção da informação dependem do tipo de atividade em que uma empresa está envolvida, bem como seu tamanho e, ainda mais importante, a cultura individual do CEO ou fundador. A segurança da informação refere-se à preservação e integridade das informações sobre uma empresa em relação a três aspectos (Sêmola, 2003):

1. Confidencialidade - as empresas procuram proteger seus dados e informações da divulgação a pessoas não autorizadas, ou seja, os dados e a informação devem ser protegidos de acordo com a necessidade de segredo e estarem disponíveis apenas para as pessoas a quem se destina;
2. Integridade - todos os sistemas de informação devem fornecer uma representação precisa dos sistemas físicos que representam, ou seja, a informação deve ser mantida sob a forma em que é disponibilizada por seu dono e deve ser protegida de alterações intencionais ou acidentais;

3. Disponibilidade - o objetivo da infraestrutura de informação da empresa é disponibilizar seus dados e informações para aqueles que estão autorizados a usá-lo, ou seja, as informações protegidas devem ser disponibilizadas sempre que necessário, mas apenas para os indivíduos a quem se destina.

As grandes empresas que acumulam informações estratégicas de enorme valor agregado também tendem a ter pessoal altamente especializado e regularmente informado sobre a necessidade de segurança da informação; essas empresas estabeleceram uma cultura envolvendo implantação e manutenção de sistemas de segurança da informação. O nível de automação alcançado pelo mercado, especialmente em relação à organização da informação, tornou necessário estabelecer uma norma específica para o gerenciamento da segurança da informação. Essas normas são originárias das normas brasileiras de Segurança da Informação que possuem os seguintes domínios (Sêmola, 2003):

- Política de segurança[1];
- Segurança organizacional;
- Classificação e controle de ativos de informação;
- Segurança pessoal;
- Segurança física e ambiental;
- Gerenciamento de operações e comunicação;
- Controle de acesso;
- Desenvolvimento e manutenção de sistemas;
- Gerenciamento da continuidade do negócio; e
- Conformidade.

As empresas menores, revelaram uma falta de coerência entre as verdadeiras necessidades e as ações preventivas efetivas tomadas para a segurança da informação. Por razões financeiras e pela falta de uma visão mais ampla do que e como proteger os ativos de segurança, essas empresas se concentram

[1] Política de segurança: é um plano de ação para enfrentar problemas de segurança ou um conjunto de regulamentos para manter um nível de segurança. Ele pode abranger qualquer coisa das práticas para garantir um único computador, para construir / segurança local, para garantir a existência de um estado-nação inteiro.

principalmente em pequenos investimentos em ferramentas tecnológicas limitadas, geralmente inadequadas para o trabalho (SINGER, 2012).

Essas empresas não têm sentido dos riscos envolvidos e, portanto, tendem a ter uma falsa sensação de segurança, dando aos seus usuários / funcionários a sensação de que eles estão seguros durante a manipulação de dados e informações, considerando que as ferramentas realmente adotadas geralmente são inadequadas e podem fornecer apenas cobertura parcial em relação à segurança (LAUDON *et al*., 2014).

É um fato que não há segurança 100% para nenhum setor, mas implementações inadequadas ou parciais são mais problemáticas em relação à segurança do computador do que a falta de um programa de segurança em acesso interno ou acesso externo à Internet, desde que os usuários estejam cientes dessa ausência. Em tal situação que envolve a falta de cobertura, os usuários podem ser orientados e treinados para serem cuidadosos, isso é muito melhor do que propagar a imagem irreal que uma empresa é segura (LAUDON *et al*., 2014).

A incapacidade de desenvolver tais programas de treinamento / conscientização aumenta a probabilidade de ataques bem-sucedidos (LAUDON *et al*., 2014). De acordo com Laudon *et al*. (2014), a maioria das pequenas empresas têm uma falta total de uma cultura de segurança. Eles tendem a ter problemas com os funcionários que acessam *sites* da Internet com conteúdo inadequado, bem como a utilização não autorizada no trabalho de comunicadores instantâneos (como *MSN*, *SKYPE*, etc.), eles também abrem *e-mails* de procedência duvidosa.

2.6 A IOT E A SEGURANÇA DE DADOS

Os principais problemas de segurança na Internet das Coisas decorrem do fato de se fornecer o terreno fértil para muitos ataques mal-intencionados (SINGER, 2012). Isso se deve principalmente ao fato de que a Internet das Coisas consiste em milhões de dispositivos interconectados, a maioria dos quais nem sempre pode ser controlada.

Isso cria brechas de segurança nos sistemas, resultando em riscos de vazamento e perda de dados ou mesmo permitindo que terceiros controlem/destruam dispositivos e infraestrutura. À medida que o número de dispositivos interconectados aumenta e sua complexidade aumenta, também

aumenta a possibilidade de atividade maliciosa sem as medidas apropriadas (ZANI, 2016).

Abordar os riscos e lacunas de segurança da IoT é fundamental e de importância para sua expansão. A segurança proporcionada pelas tecnologias IoT é o fator mais determinante para que tais tecnologias sejam amplamente adotadas pelos usuários finais. Se não houver garantias quanto à confidencialidade no nível do sistema, identificação e privacidade dos membros interessados, nenhuma solução de IoT prosperará (VALENTE, 2011).

Os dispositivos da Internet das Coisas (IoT) carregam uma variedade de riscos. O risco de que as informações pessoais dos usuários de um sistema sejam comprometidas, que o acesso não autorizado a dispositivos possa ser obtido ou que vários outros sistemas possam ser atacados é parte integrante da Internet das Coisas não apenas hoje, mas também no futuro, com as taxas de crescimento que se seguem, é muito possível que a Internet das coisas levará a um grande aumento no número de violações de dados e, portanto, as medidas de segurança e proteção desses dados devem aumentar de acordo (SCHNEIER, 2007).

Os ataques a dispositivos conectados podem levar a riscos terríveis que ameaçam a existência física até mesmo dos próprios usuários dessa tecnologia, não apenas dos dispositivos que estão sendo usados. Por exemplo, os dispositivos médicos podem ser modificados para relatar diferentes indicações, ou até mesmo mecanismos específicos de um carro podem ser adulterados para obter controle sobre o sistema de freio e sistema de navegação e direção do veículo (DE OLIVEIRA, 2018).

Se considerar que em poucos anos a tecnologia dos veículos automotores também aumentará significativamente, dá para entender o volume e a gravidade do problema. Porque se vulnerabilidades e falhas de segurança forem encontradas em tais dispositivos e máquinas por *cibercriminosos*, além dos esperados acidentes e congestionamentos de trânsito, vidas humanas também estão muito ameaçadas. No entanto, o risco não é atribuído apenas aos invasores que obtêm o controle dos dispositivos conectados, mas também à vasta e crescente quantidade de dados coletados e armazenados diariamente por objetos inteligentes (FENN e LEHONG, 2015).

Dispositivos com capacidade de coletar uma grande quantidade de dados estão gradativamente sendo cada vez mais utilizados em diversas áreas do

cotidiano das pessoas, como a casa, o carro e o local de trabalho. Isso resulta em enormes quantidades de dados sendo criados, processados e armazenados, criando assim o terreno certo para o fácil uso indevido de dados por terceiros (DOURADO, 2013).

Com base em vários incidentes perigosos de *hackers* de dispositivos e interceptação de dados que foram observados no setor de saúde, em veículos conectados à Internet, mas também em jogos eletrônicos, percebe-se que o estabelecimento de fortes medidas de segurança em sistemas de Internet das coisas é uma questão crítica (CHAGAS, 2014). São exemplos típicos de riscos e falhas de segurança na IoT (Jansen et al., (2013):

1. *Transmissão de dados com criptografia fraca ou sem criptografia*: A maioria dos dispositivos utilizados na Internet das Coisas não possui o poder de processamento necessário ou o *software* adequado para realizar cálculos complexos, como a aplicação de algoritmos poderosos para comunicação segura ou criptografia de dados. Assim, os dados coletados são transmitidos sem criptografia e, como resultado, são facilmente violados por terceiros.
2. *Certificação e autorização insuficientes*: Baixos requisitos para criar senhas fortes, uso descuidado de senhas e não alteração de senhas regularmente podem levar a medidas de autenticação fracas, colocando todo o sistema da Internet das Coisas em risco.
3. *Contato online inseguro*: As credenciais usadas são fracas.
4. *Uso de software inseguro*: Devido à sua natureza de processamento fraca, a maioria dos dispositivos IoT não foi projetada para aceitar atualizações e *upgrades* de *software*. Isso tem como consequência tornar extremamente difícil eliminar uma vulnerabilidade enquanto nenhuma atualização for feita.

2.7 A ISO 27001

A ISO/IEC 27001 faz parte da família de normas ISO/IEC 27000 publicada pela Organização Internacional de Normalização (ISO) e pela Comissão Eletrotécnica Internacional (IEC) (REVISÃO DE SEGURANÇA, 2013). O Regulamento Geral de Proteção de Dados não dá instruções claras sobre como a segurança dos dados será implementada, mas transfere a responsabilidade para a

entidade individual, a certificação ISO 27007 é uma boa prática para as entidades construírem as medidas de segurança dos dados que gerenciam (LAUDON, 2014).

A ISO/IEC 27001 define um sistema de gestão destinado a colocar a segurança da informação sob controle de gestão e fornece requisitos específicos. As organizações que atendem aos requisitos podem ser certificadas por um organismo de certificação credenciado após a conclusão bem-sucedida de uma auditoria. Este padrão internacional é o único padrão que define os requisitos de um sistema de gerenciamento de segurança da informação (ZANI, 2016).

Ou seja, ao implementar a ISO 27001, a organização desenvolverá um ISMS (sistema de gestão de segurança da informação): um sistema integrado à organização e continuamente monitorado, atualizado e controlado. Ao utilizar um processo de melhoria contínua, a organização é capaz de garantir que o sistema se adapte às mudanças - tanto no ambiente quanto dentro da organização - para identificar e reduzir continuamente os riscos. De acordo com a norma, o sistema oferece os seguintes benefícios (Patel, 2020):

- Ele fornece a capacidade de detectar e isolar rapidamente quaisquer violações de segurança;
- Pode ser aplicado por todos os órgãos ou organizações, independentemente do tamanho, tipo ou objeto;
- Estabelece os controles gerais necessários para as inspeções;
- Garantia de que a integridade dos sistemas, sistemas de processamento e informações seja mantida; e
- Demonstra a existência de um sistema de gestão de segurança da informação formal e operacional.

Assim, com a sua aplicação, o Regulamento Geral de Proteção de Dados traz as seguintes alterações na gestão, tratamento, armazenamento e segurança geral dos dados pessoais (Patel, 2020):

1. Direitos aprimorados dos titulares de dados: O titular dos dados passou a ter direitos acrescidos que incluem o direito ao esquecimento, direito à restrição do tratamento, direito à retificação, direito à portabilidade, obrigação de notificação em caso de violação;

2. Notificação de violação de dados: O responsável pelo tratamento de dados deve, em caso de violação, informar no prazo de 72 horas a Autoridade de Proteção de Dados Pessoais e, em alguns casos, o próprio titular;
3. Proteção de dados por *design* e por padrão: O controlador deve aplicar, tanto no momento da determinação dos meios de processamento quanto no momento do processamento, medidas técnicas e organizacionais adequadas para atender aos requisitos deste regulamento e proteger os direitos dos titulares de dados;
4. Reforço das condições para a prestação de consentimento dos dados subjacentes: Quando o tratamento se basear no consentimento do titular, deve agora ser explícito e com pleno conhecimento disso e, além disso, é fornecido com a possibilidade de revogação;
5. Avaliação do impacto da proteção de dados: Nos casos em que o tratamento possa implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deve efetuar, antes do tratamento, uma avaliação do impacto das operações de tratamento previstas na proteção dos dados pessoais;
6. Manter registros das atividades de processamento: Cada controlador deve manter um registro das atividades de processamento pelas quais é responsável; e
7. Designação do Encarregado da Proteção de Dados: É definido o cargo de *Data Protection Officer* (DPO), que em muitos casos se torna obrigatório.

Os invasores, no caso de tal falta de segurança, podem não apenas acessar os dados, mas também alterá-los, excluí-los ou até mesmo controlar os dispositivos conectados e negar o acesso a usuários "legítimos". Por sua vez, desenvolvedores e *designers* de interface podem verificar a segurança da interface das seguintes maneiras (Murillo, 2012):

- Exigir que o usuário altere as credenciais padrão na configuração inicial da conta ou instalação do programa;
- A existência de um mecanismo para bloquear o perfil do usuário após um determinado número de tentativas de *login* malsucedidas;

- Mecanismo de recuperação de senhas de usuários ativos por meio de identificação em dois níveis e evitando a criação de um novo usuário com a mesma informação ativa; e
- Controle do *software* de interface para que haja proteção contra *scripting cross-site*, falsificação de solicitação *cross-site* e injeção de sql.

Muitos problemas com a criptografia de dados das IOTs em trânsito são fáceis de detectar monitorando o tráfego de rede e procurando dados legíveis. Existem ferramentas automatizadas disponíveis que buscam a implementação correta da criptografia de transporte conhecida (criptografia de transporte comum), como SSL e TLS (PEIXOTO, 2010).

O "dano" que pode ser causado por tal falta de proteção é a possível perda de dados. Os dados interceptados podem permitir que terceiros exponham totalmente os dispositivos ou contas dos usuários. Devem ser feitas verificações para determinar se há falta de criptografia durante a transferência de dados ou não, são as seguintes (Raymond, 2004):

- Para rastrear os movimentos de dispositivos na rede, aplicativos móveis e qualquer conexão de nuvem para garantir que nenhuma informação seja trafegada em texto simples;
- Investigue se os protocolos SSL ou TSL estão atualizados e implementados adequadamente; e
- Investigar se o uso de protocolos de criptografia específicos é recomendado e aceitável.

Em conclusão e de acordo com o que foi mencionado acima, para garantir que a criptografia durante a transferência de dados existe e é suficiente, deve (Patel, 2020):

- Os dados precisam ser criptografados em trânsito pela rede usando protocolos como SSL e TLS;
- Se os protocolos SSL ou TLS não forem usados, alguma outra técnica de criptografia deve ser usada para proteger os dados enquanto eles trafegam pela rede; e

- Usar apenas mecanismos de criptografia comumente aceitos e evitar protocolos de criptografia proprietários.

Onde problemas de privacidade são identificados, a ameaça decorre da possibilidade de que os dados coletados não sejam devidamente protegidos ou coletados sem uma necessidade real, se é que são coletados. O acesso por terceiros no caso de um ataque malicioso pode ser devido ao seguinte (Patel, 2020):

- O método de autenticação insuficiente ou verificação de autenticação;
- A falta de criptografia durante a transferência de dados; e
- A existência de serviços de rede inseguros.

Os que podem realizar tal ataque podem ser usuários internos ou externos, que tenham acesso a um dispositivo individualmente ou à rede à qual está conectado, a um aplicativo para dispositivo móvel (aplicativo móvel), a uma conexão em nuvem (*cloud*) (KUROSE, 2011).

A falta de proteção de dados resulta da recolha de dados pessoais sem que esta seja necessariamente exigida e ainda da falta de proteção adequada. Essa falha de segurança é fácil de detectar simplesmente revisando os dados coletados durante a ativação de um dispositivo pelo usuário. Também existem ferramentas automatizadas que têm a capacidade de procurar padrões específicos nos dados que possam indicar uma possível coleta de dados pessoais ou outros dados confidenciais (INTEL, 2021).

Finalmente, com a implementação do Regulamento Geral de Proteção de Dados e a certificação segundo a norma ISO 27001, a proteção e uso adequado dos dados torna-se uma prática comum e um procedimento necessário para todas as organizações e sistemas. As verificações que devem ser feitas para determinar se existe ou não uma forma de expor os dados pessoais a terceiros são as seguintes (Intel, 2021):

- Determinar todos os tipos de dados coletados pelo dispositivo, aplicativo móvel e qualquer interface de nuvem para determinar se a coleta é necessária e, em caso afirmativo, os dados estão seguros;

- Apenas os dados necessários devem ser coletados de um dispositivo ou *software*;
- Verifique se as informações pessoais podem ser expostas durante o armazenamento ou transmissão em uma rede ou na Internet quando não estão devidamente criptografadas;
- Se estiver claro quem tem acesso às informações pessoais que foram coletadas;
- Determinar se os dados coletados podem ser identificados ou não;
- Para determinar se os dados coletados são realmente necessários para a operação específica do dispositivo e se o usuário final tem a escolha e a informação de que essa coleta de dados está ocorrendo;
- Para determinar a política de retenção de dados e as informações corretas dos usuários.

Em conclusão, por parte do desenvolvedor-administrador do dispositivo ou sistema, as seguintes ações devem ser tomadas para garantir a integridade dos dados pessoais coletados e processados, bem como sua proteção (Fleck e Dimov, 2012):

- Apenas os dados necessários são coletados, o que é necessário para a funcionalidade de um sistema ou dispositivo;
- Os dados coletados devem ser o menos sensíveis possíveis;
- Os dados coletados devem ser desidentificados ou anônimos;
- Os dados coletados são protegidos com métodos de criptografia adequados;
- Cada dispositivo e as partes de um sistema devem proteger adequadamente os dados pessoais que coletam e mantêm;
- Somente pessoas autorizadas podem acessar as informações pessoais coletadas;
- Ter definido limites de retenção para os dados coletados e cumpri-los; e
- Os usuários finais devem ter a possibilidade de recusar a coleta e atualização dos dados que já possuem, quando isso for necessário para o funcionamento do dispositivo.

A responsabilidade pela operação segura dos dispositivos e pela preservação das informações diz respeito principalmente aos projetistas dos dispositivos e aos desenvolvedores do *software*, mas aos usuários finais. É o usuário quem julgará com base nas especificações de um sistema se o utilizará porque atende às suas necessidades e se confiará seus dados a ele (BALLONI, 2006).

Existe também em muitos casos a metodologia para que o próprio usuário possa verificar por si mesmo, sem a necessidade de conhecimentos especializados ou *softwares* complexos, se o produto que está utilizando não possui brechas de segurança. Especialmente neste último caso, o da segurança física, o usuário pode proteger seus dispositivos e dados usando credenciais fortes e sempre sabendo a localização de seus dispositivos, caso sejam portáteis (CDBI, 2011).

3. ANÁLISE E DISCUSSÃO DOS RESULTADOS

Com mais de 100 milhões de usuários de Internet a partir de 2015 (MINIWATTS, 2015), o Brasil viu suas taxas de acesso à Internet aumentar substancialmente ao longo da última década, incluindo o uso de telefones celulares. No entanto, o Brasil está atrasado na legislação em relação ao que os dados precisam ser protegidos, bem como especificações sobre como os dados devem ser protegidos.

As leis de crimes cibernéticos 12.735 e 12.737 que foram introduzidas em 2013 são um excelente ponto de partida para o Brasil e são as primeiras leis aprovadas especificamente em relação à criminalidade informática (COSTA, 2014). O Brasil precisa definir o que eles consideram dados pessoais e dados pessoais sensíveis, bem como especificar regulamentos sobre como proteger tais dados. De acordo com Costa (2014) a legislação pendente, se aprovada, será um avanço significativo para essas áreas e deve dar ao Brasil seu primeiro quadro sólido de proteção de dados e regulamentos de segurança.

4. CONCLUSÃO

A Internet das Coisas é uma das tecnologias mais difundidas desse tempo. A penetração da Internet e o uso de redes na vida cotidiana tornou-se parte integrante dela, pois as áreas em que é aplicada dizem respeito à totalidade das atividades da pessoa média no mundo ocidental. Mas à medida que encontram aplicações em áreas como saúde, transporte, energia, comércio, cidades inteligentes e casas inteligentes, a questão da segurança é mais relevante do que nunca.

Com a rápida aceleração da evolução das ligações globais e dispositivos móveis, toda esta tecnologia tornou-se disponível a uma tal velocidade que a familiaridade com a tecnologia veio antes de estar totalmente amadurecida e todas as falhas de segurança e potenciais riscos foram identificados. Ou seja, esta tecnologia está a ser desenvolvida e testada no utilizador final o que, embora seja uma inovação em certo sentido, levanta grandes preocupações com a segurança dos dados e dispositivos.

Contra ações maliciosas ela ganha maior peso quando falam até mesmo da chamada guerra eletrônica. Com tantos dispositivos interconectados que cada um possui e interage uns com os outros todos os dias, um possível ataque cibernético pode agora atingir estados e grandes organizações. Com a implementação do Regulamento Geral de Proteção de Dados, foi dado um grande passo no sentido da proteção da informação e da vigilância relativamente à mesma.

5. REFERÊNCIA

ATZORI, L., Iera, A. e Morabito, G. **A Internet das Coisas: Uma pesquisa. Redes de Computadores,** 54 (15), p.27-28, 2010.

BALLONI, Antonio José, **por que GESITI?** Edit. Komedi; 2006.

BORGIA E. **A visão da Internet das Coisas: Principais recursos, aplicativos e questões abertas**, Computer Communications, 54 (1), p.1-31, 2014.

CHAGAS, Fernando Celso Dolabela – **O Segredo de Luíza**. Cultura Editora Associadas, 2014.

COMITÊ DIRETOR BRASILEIRO DE INTERNET (CDBI). **Pesquisa sobre o Uso de Tecnologias de Informação e Comunicação no Brasil e no mundo**, 2011 - HABITAÇÕES TIC E ENERCAS DE TIC. Disponível em: <www.cgi.br>. Acesso em: 20 dez. 2022.

COSTA, L. **Uma breve análise da lei de proteção de dados no Brasil**. 2014. Disponível em: <http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/Report%20(June%204th%202>. Acesso em: 02 jan. 2023.

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.

DOURADO, E. **Vamos construir uma internet mais segura**. New York Times, 2013. Disponível em:<http://www.nytimes.com>. Acesso em: 11 mai. 2022.

FENN, LM; LEHONG, AP. **Computação Ubíqua e Inteligência Ambiental**. Detectando, processando e usando informações ambientais JM García-Chamizo, G. Fortino e SF Ochoa, editores, Cham: Springer International Publishing. p.16-121, 2015.

FLECK, B. e DIMOV, J., **Pontos de acesso sem fio e envenenamento por ARP**, Cigital, Inc., 2012.

FLOERKEMEIER, C., LAMPE, M. e RODUNER, C. **Facilitando o desenvolvimento de RFID com a Plataforma de Prototipagem Accada**. In: PerCom 2007. White Plains, NY, EUA: IEEE Computer Society, p. 495-500, 2007.

GARTNER, M. **Ciclo *Hype* para a Internet das Coisas**, 2016., p.16-18, 2016.

IBGE, Instituto Brasileiro de Geografia e Estatística. **Estimativa da População, 2017**. Disponível em: <https://ww2.ibge.gov.br/apps/populacao/projecao/index.html>. Acesso em: 01 jan. 2023.

INTEL. **Segurança de IoT**. 2021. Disponível em: https://www.intel.com.br/content/www/br/pt/design/technologies-and-topics/iot/security.html/. Acesso em: 15 dez. 2022.

JANSEN, T., HINZPETER, B. & SCHWARZBART, P. **Alemanha. Leis de proteção de dados do mundo, 2013.** 30, 99- 104. Disponível em: <http://www.dlapiper.com/files/Uploads/Documents/Data-Protection-Laws-of-the-World-Handbook-Second-Edition-2013.pdf>. Acesso em: 03 dez. 2022.

KUROSE, J. F. e ROSS, K. W., **Redes de Computadores: Uma Abordagem Top-Down com a Internet,** Addison Wesley, 2011.

LAUDON, Kenneth et al.MIS: ***Managing the Digital Firm Active Book***,ed. Pearson – Prentice Hall – 2014.

MADAKAM, S., Ramaswamy, R. e Tripathi, S., 2015. **Internet das Coisas (IoT): Uma Revisão de Literatura. Jornal de Computação e Comunicações**, 3 (5), p.164–173, 2015.

MAZHELIS, O. et al. **Mercado de Internet das Coisas, Redes de Valor e Modelos de Negócios: Estado do relatório de arte**, IEEE Internet of Things Journal. p.18-45, 2013.

MURILLO, N. M. de O., **Segurança Nacional**, Novatec Editora Ltda., 2012.

OLIVEIRA, S. **Nuvem de Coisas para Sensing-as-a-Service: Arquitetura, Algoritmos e Caso de Uso**. IEEE Internet of Things Journal, 3 (6), p.10-111, 2013.

PATEL, Rushabh. IoT and home automation: What does the future hold? IoT Now, 2020. Disponível em: <https://www.iotnow.com/2020/06/10/98753-iot-homeautomation-future-holds>. Acesso em: 16 nov. 2022.

PEIXOTO, Mário C. P. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2010.
RAYMOND, McLeod et al. "***Managing Information Systems***" Prentice Hall – 2004.

REVISÃO DE SEGURANÇA. **Regulamento da Comissão (CR 611/2013) sobre as medidas aplicáveis à notificação de violações de dados pessoais, 2013**. Disponível em: <http://eur-lex.europa.eu/legal-content / EN / TXT / PDF /? Uri = uriserv: OJ.L_.2013.173.01.0002.01.ENG>. Acesso em: 02 dez. 2022.

ROSE K., ELDRIDGE S., CHAPIN L. **A Internet das Coisas (IoT): Uma Visão Geral - Entendendo as Questões e Desafios de um Mundo Mais Conectado**, Internet Society. 2015.

SINGER, Talyta. **Tudo conectado**. Salvador. ed. Simsocial, 2012.

TIMM, I. J. **Gestão Estratégica de Sistemas Autônomos de Software: Artigo de Visão Geral, Relatório Técnico 35**, Universidade de Bremen, Centro de Computação e Tecnologias de Comunicação, 2006.

SCHNEIER, Bruce Segurança.com: **Segredos e mentiras sobre a proteção na vida digital**. São Paulo: Editora Campus, 2007.

SEBRAE. **Conheça melhor o ambiente das micro e pequenas empresas, 2017.** Disponível em: <http://www.sebrae.com.br/sites/PortalSebrae/estudos_pesquisas/conheca-melhor-o-ambiente-das-micro-e-pequenas-empresasdestaque19,d6a2f925817b3410VgnVCM2000003c74010aRCRD>. Acesso em: 01 nov. 2022.

SÊMOLA, Marcos. **Gestão da Segurança da Informação, uma visão executiva.** Rio de Janeiro: Editora CAMPUS, 2003.

SINGHAL, S. K., **Entendendo a segurança da LAN sem fio**, ReefEdge, 2007.

VALENTE, Bruno Alexandre Loureiro. **Um middleware para a Internet das coisas**. 2011.

ZANI, Bruno. **As vulnerabilidades e necessidades de segurança em IoT**. 2016. Disponível em:<http://www.securityreport.com.br/overview/mercado/vulnerabilidadesnecessidades-seguranca-iot/#.XOSDjMhKjIU> Acesso em: 10 dez. 2022.