Centro Universitário do Planalto Central Apparecido dos Santos - UNICEPLAC
Curso de Sistemas de Informação
Trabalho de Conclusão de Curso

Segurança em IoT

Gama-DF
2021

(61) 3035-3900
www.uniceplac.edu.br
Área Especial para Indústria
Lote nº 02, Bloco A, Sala 304,
Setor Leste, Gama, Brasília, DF
CEP 72.445-020

ANDRÉ FERREIRA ALMEIDA DE CARVALHO
CHRISTYAN MATTEUS LIMA SANTOS
LUCAS VAZ GONÇALVES

Segurança em IoT

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Sistemas de Informação pelo Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac.

Orientador: Prof. Esp. Hélder Line Oliveira

Gama-DF

2021

ANDRÉ FERREIRA ALMEIDA DE CARVALHO
CHRISTYAN MATTEUS LIMA SANTOS
LUCAS VAZ GONÇALVES

Segurança em IoT

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Sistemas de Informação pelo Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac.

Gama, 15 de junho de 2021.

Banca Examinadora

Prof. Nome completo
Orientador

Prof. Nome completo
Examinador

Prof. Nome Completo
Examinado

Segurança em IoT

André Ferreira Almeida de Carvalho

Christyan Matteus Lima Santos

Lucas Vaz Gonçalves

Resumo:

Com o grande número de dispositivos conectados coletando informações pessoais, as preocupações das organizações com a segurança da Internet das Coisas (IoT) ficaram recorrentes. Sendo assim, este artigo tem por objetivos: caracterizar a Internet das Coisas (IoT); discorrer sobre a segurança da informação e privacidade de dados; citar os princípios da segurança de informação; mencionar empresas que trabalham com IoT, apresentar as boas práticas e como elas tratam a segurança dos dados. Nesse caso, a pesquisa torna-se relevante porque as ferramentas usadas pelas corporações devem ser testadas e avaliadas ativamente para alcançar um desenvolvimento na área de tecnologia da informação. Também objetiva questionar a importância da privacidade de dados pessoais no padrão da IoT e demonstrar suas inferências implícitas sobre a conformidade dos usuários com essa nova tecnologia. Em vista dessa situação, presume-se que apesar de todas as boas práticas e mecanismos de defesa, ainda são necessárias que novas pesquisas na área de segurança sejam desenvolvidas, a fim de aumentar ainda mais a efetividade da segurança, por conta do enorme crescimento dessa tecnologia que, junto com novas oportunidades, abre uma "janela" de ataque para "*cyber*" criminosos.

Palavras-chave: Organizações; Segurança da Informação; Tecnologia da informação; Mecanismos de defesas; Internet das Coisas.

1 INTRODUÇÃO

A primeira menção de "*Internet of Things*", Internet das Coisas (IoT), propriamente, só aparece em 2001 no livro branco de Brock, pesquisador do Auto-ID Center (BROCK, 2001). Entretanto, Kevin Ashton, outro pesquisador do Auto-ID Center, reclama para si a paternidade do termo. Ashton diz que em 1999, propôs o termo quando realizava uma apresentação sobre radiofrequência em rede (ASHTON, 2009; UCKELMANN et al, 2011). Na abertura da *IoT Week* 2013 (Conferência internacional anual que reúne representantes da indústria e das instituições de todo o mundo, onde plataformas, serviços e aplicações industriais são discutidos.) com uma mensagem de vídeo pré-gravada, Ashton insistiu na compreensão de que a IoT está aqui agora, não é o futuro, mas o presente.

De acordo com pesquisa da Accenture, uma empresa multinacional de consultoria de gestão, tecnologia da informação e outsourcing, a Internet das Coisas tem potencial para contribuir com US $14,2 trilhões da produção mundial até 2030.

No entanto, como os dispositivos estão conectados, eles também enfrentam a ameaça de ataques cibernéticos. O artigo "Um guia para LGPD (Lei geral de proteção de dados pessoais) (2018)" diz que, para a indústria os riscos de violações de segurança de dados são gravíssimos, cujas consequências incluem o comprometimento da implementação do projeto e a falência da empresa.

Segundo a NTT Ltd. (companhia global de serviços de tecnologia, 2021), em seu Relatório de Inteligência de Ameaças Globais 2021 (GTIR), revela como os cibercriminosos estão tirando proveito da desestabilização global visando indústrias essenciais e vulnerabilidades comuns da mudança para o trabalho remoto. Os setores de Saúde, Finanças e Manufatura viram um aumento nos ataques (200%, 300% e 53%, respectivamente), com esses três setores principais respondendo por um total combinado de 62% de todos os ataques em 2020, um aumento de 11% em relação a 2019.

Outro exemplo que demonstra a necessidade de que se estude a respeito da segurança

(61) 3035-3900
www.uniceplac.edu.br
Área Especial para Indústria
Lote nº 02, Bloco A, Sala 304,
Setor Leste, Gama, Brasília, DF
CEP 72.445-020

aplicada à Internet das Coisas, é devido ao distanciamento social, que levaram a uma inundação inesperada de dispositivos nas redes, resultando em um aumento de ameaças potenciais para as empresas que lutam para se manterem operacionais durante a pandemia. Os pesquisadores do SonicWall Capture Labs (2020), pioneiros no uso de inteligência artificial para pesquisa e proteção de ameaças há mais de uma década, encontraram um aumento de 30% nos ataques de *malware* IoT, um total de 32,4 milhões em todo o mundo.

A maioria dos dispositivos IoT, incluindo dispositivos inteligentes ativados por voz, campainhas, câmeras de TV e eletrodomésticos não foram projetados tendo a segurança como prioridade. Isso torna os dispositivos IoT suscetíveis a ataques, fornecendo aos criminosos digitais vários pontos de entrada.

O presente trabalho busca discorrer sobre IoT, visando os protocolos de segurança e integridade dos dados, levando em consideração a Lei Geral de Proteção de Dados Pessoais (LGPD; Redação dada pela Lei n° 13.853, de 2019).

1.1 OBJETIVOS

1.1.1 Objetivo geral

Analisar conceitualmente as configurações de segurança e privacidade implementadas por organizações que utilizam IoT em seus negócios.

1.1.2 Objetivos específicos

Caracterizar a Internet das Coisas (IoT); discorrer sobre segurança da informação e privacidade de dados; citar os três princípios da segurança da informação; mencionar empresas que trabalham com IoT e falar sobre suas boas práticas e como tratam a segurança; apontar se as empresas em um âmbito geral, estão prontas para essa tecnologia.

(61) 3035-3900
www.uniceplac.edu.br
Área Especial para Indústria
Lote nº 02, Bloco A, Sala 304,
Setor Leste, Gama, Brasília, DF
CEP 72.445-020

2 REVISÃO DE LITERATURA

A ideia de uma rede mundial de dispositivos conectados que trocam informação entre si é bastante ampla e faz com que muitas tecnologias e aplicações diferentes atendem pelo nome de Internet das Coisas.

Os dispositivos com tecnologia IoT, podem receber e enviar dados, como também ser apenas um emissor, transmitindo alguma informação sem receber nada. O envio de dados pode ser feito em intervalos predeterminados, muitas vezes minuto a minuto, ou contínuo, entretanto é recebido apenas quando alguém passa por ele, neste caso o objeto é chamado de farol.

Podem ser apenas receptores, quando conectado exibe informações que recebem da rede à que está conectado. Há objetos que coordenam suas ações, conectando-se uns aos outros, em vez de conectados separadamente a um ponto central, podendo coordenar para se moverem juntos, realizarem uma ação comum ou trocar dados.

A diversidade dos recursos tecnológicos, integram e viabilizam a utilização da IoT em diversos espaços físicos, assim a classe é composta por dois blocos, identificação e serviços. A identificação é primordial para detectar os objetos que serão utilizados para conectá-los à Internet. Entre esses identificadores destaca-se RFID, NFC (*Near Field Communication*) e endereçamento IP. Os sensores (Atuadores), ficam com a responsabilidade de coletar informações, armazenar e/ou encaminhar os dados para as bases de dados, clouds ou data centers.

O crivo da Comunicação, é referente às técnicas de conexão dos objetos, com o importante papel no consumo de energia, normalmente são utilizadas: WiFi (padrão de LAN sem fio, parte do IEEE 802.11, para comunicação entre diferentes dispositivos), Bluetooth **(t**ecnologia de comunicação sem fio que interliga e permite a transmissão de dados entre dispositivos através de ondas de rádio), IEEE 802.15.4 (padrão que especifica a camada física e efetua o controle de acesso para redes sem fio pessoais de baixas taxas de transmissão) e RFID (*radio frequency identification* são as tecnologias que utilizam a frequência de rádio para captura de dados). E referente à

(61) 3035-3900
www.uniceplac.edu.br
Área Especial para Indústria
Lote nº 02, Bloco A, Sala 304,
Setor Leste, Gama, Brasília, DF
CEP 72.445-020

configuração da computação, está incluído a unidade de processamento, microcontroladores, processadores e os *field-programmable gate array* (FPGAs), responsáveis por executar algoritmos locais nos dispositivos. De acordo com MAXFIELD et al. (2004):

> Um FPGA é um dispositivo lógico programável, apresentado como circuito integrado, que contém matrizes de blocos lógicos, com interconexões configuráveis, chamados CLBs (*Configurable Logic Blocks*), organizados de tal maneira que um desenvolvedor possa programá-los para executar uma ampla gama de tarefas. (MAXFIELD, 2004).

O bloco de Serviços, tem a missão de prover diversas classes de serviços, entre elas, serviços de identificação, que é responsável por mapear as entidades físicas nas virtuais, como temperatura, coordenadas gráficas; Serviços de Agregação de Dados, utilizados para coletar e totalizar dados obtidos a partir dos dispositivos; Serviços de Colaboração e inteligência, cuja a ação é sobre os serviços de agregação de dados, possibilitando a tomada decisões e a reação de modo adequado, conforme determinado cenário; Serviços de Ubiquidade, tem a finalidade específica de prover serviços de colaboração e inteligência há todo momento, independente do lugar.

O Wi-Fi é a solução mais comum para a comunicação sem fio, em relação ao padrão Ethernet (IEE 802.3). Baseado na especificação do protocolo IEEE 802.15.4 para a camada de enlace, suas características são de baixa vazão, reduzido consumo energético e baixo custo. Cabe destaque especial para os padrões tecnológicos da telefonia celular 3G/4G, muito utilizado na IoT, podem alcançar grandes distâncias, aproveitando a infraestrutura das redes de telefonia celular. Conforme a Tabela 1, pode-se observar a tecnologia e suas características.

(61) 3035-3900
www.uniceplac.edu.br
Área Especial para Indústria
Lote nº 02, Bloco A, Sala 304,
Setor Leste, Gama, Brasília, DF
CEP 72.445-020

Tabela 1 - Comparação das tecnologias da comunicação

Protocolo	Alcance	Frequência	Taxa	IPv6	Topologia
Ethernet	100/2000 m	N/A	10 Gbps	Sim	Variada
Wi-Fi	50 m	2.4/5 GHz	1300 Mbps	Sim	Estrela
BLE	80 m	2.4 GHz	1 Mbps	Sim*	Estrela/Mesh
ZigBee	100 m	915 MHz/2.4 GHz	250 kbps	Sim	Estrela/Mesh
3G/4G	35/200 km	1900/2100/2500 MHz	1/10 Mbps	Sim	Estrela
SigFox	10/50 km	868/902 MHz	10–1000 bps	–	–
LoraWan	2/5 km	Sub-GHz	0.3-50 kbps	Sim	Estrela

Fonte: homepages.dcc.ufmg.br

A modelagem de dados coletados por sensores, raramente possui uma padronização hierárquica (relacionamentos ou mesmo um formato padrão) para sua utilização, assim os softwares de modelagem permitem utilizar esses dados de forma compatível e interoperabilidade, ajustando-os para formatos de padrões interpretáveis. O real objetivo da modelagem é definir um padrão, unificando os atributos e características conforme o domínio da aplicação.

Suas representações são *key-value, markup scheme, graphical, object based, logic-based* e *ontology-based modeling*. Já a sua aplicabilidade tem uma variação de acordo com o domínio da aplicação. Conforme (BETTINI, 2010), afirma “A representação dos dados é modelada como um conjunto de chaves e valores em arquivos de texto, e a representação da informação possui complexidade de organizar e recuperar quando o volume de dados aumenta”.

Tendo em vista, que todos os dispositivos têm ou terão acesso à Internet, como por exemplo as TV’s, geladeiras, automóveis, entre outros, fará com que se produza uma quantidade enorme de dados, que consequentemente serão armazenados em bancos de dados e, de acordo com as políticas de segurança aplicadas, poderão deixar portas abertas para ataques. A gravidade dessa situação é potencializada quando se trata de pessoas físicas, usando equipamentos pessoais. A LEI Nº 13.709,

(61) 3035-3900
www.uniceplac.edu.br
Área Especial para Indústria
Lote nº 02, Bloco A, Sala 304,
Setor Leste, Gama, Brasília, DF
CEP 72.445-020

DE 14 DE AGOSTO DE 2018, Lei de Proteção de Dados (LGPD), corrobora:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A automação residencial tem vários níveis de complexidade. Podendo comprar eletrodomésticos mais tecnológicos ou até integrar sua casa inteira para ser comandada pela fala.

Figura 1 - Smart House

Fonte: Google Imagens

Conforme mostra a figura 1, há diversos aparelhos, e tudo depende do quanto deseje tornar a *Smart House* mais conectada, inteligente e automatizada. Tudo acontece de maneira instantânea e rápida. Começa tendo uma boa conexão de internet, logo em seguida entram as assistentes virtuais, que auxiliam na execução de tarefas. Com controles universais e aparelhos compatíveis com a tecnologia de infravermelhos, esse fluxo torna possível ligar uma caixa de som apenas com a fala ou comandado por controle remoto.

(61) 3035-3900
www.uniceplac.edu.br
Área Especial para Indústria
Lote nº 02, Bloco A, Sala 304,
Setor Leste, Gama, Brasília, DF
CEP 72.445-020

Esse processo permite a predefinição de modos específicos mais utilizados no dia a dia, por exemplo, avisar para a assistente virtual que chegou em casa e ela acender as luzes do cômodo, ligar a TV no canal preferido e acionar um som ambiente automaticamente, como um padrão predefinido para a sua chegada. A maioria desses serviços também permite controle através do celular ou tablet, o que torna os riscos imensuráveis.

Se para pessoas físicas a probabilidade de risco é maior, no caso corporativo os prejuízos são incalculáveis, conforme (AYOYAN, 2015), orienta:

> Há algum tempo, as infraestruturas empresariais móveis eram bastante simples, dispositivos Blackberry eram a novidade. Em seguida, graças ao 32 lançamento de smartphones populares e da "consumerização de TI", alguns funcionários iniciantes começaram a utilizar seus próprios smartphones, tablets e outros dispositivos pessoais no trabalho. Logo, todo mundo aderiu à prática. O BYOD tornou-se generalizado, apesar de uma série de novas dores de cabeça para as empresas antes de finalmente chegarem a um consenso. (AYOYAN, 2015).

Riscos e vulnerabilidades tornam-se cada vez mais comuns, principalmente por erros cometidos por fabricantes de dispositivos que ainda não estão familiarizados com as práticas de segurança, por não acompanhar a constante e veloz evolução da Internet das Coisas, como por exemplo adicionando as funcionalidades do protocolo de internet (IP) a seus dispositivos, com o objetivo de obter maiores informações, ou no caso dos níveis de privilégios, estabelecendo senhas padrões.

3 SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS

Para a implementação da Internet das Coisas ainda é necessário resolver vários problemas para que se torne uma realidade segura em um futuro próximo. Para os problemas encontrados, são propostas algumas soluções que precisam de novas tecnologias para atender às especificidades, enquanto outras, só precisam da tecnologia existente para se adaptar ao cenário. Sobre questões de segurança e privacidade da informação, acredita-se que os dados na Internet das Coisas sejam capazes de usar a maioria das soluções já existentes neste novo paradigma.

(61) 3035-3900
www.uniceplac.edu.br
Área Especial para Indústria
Lote nº 02, Bloco A, Sala 304,
Setor Leste, Gama, Brasília, DF
CEP 72.445-020

3.1 SEGURANÇA DA INFORMAÇÃO

Segundo a PUC, Pontifícia Universidade Católica (2017):

> A Segurança da Informação (SI) é a disciplina dedicada à proteção das informações de forma a garantir a continuidade dos negócios, minimizando os danos e riscos que possam prejudicar os serviços da Instituição. Portanto, é fundamental que todos os integrantes, seja da área administrativa ou dos núcleos de docentes ou discentes, pratiquem e disseminem a segurança digital.

Para Alves (2006, p. 15), a Segurança da Informação "visa proteger a informação de forma a garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócios".

A segurança da informação busca proteger os ativos de uma empresa ou indivíduo com base na preservação de alguns princípios. Os três princípios considerados centrais ou principais, mais comumente analisados são: confidencialidade; integridade e disponibilidade. Eles formam o que chamamos de pirâmide de segurança da informação sendo possível encontrar a sigla **CID** para referenciar estes princípios.

3.1.1 Confidencialidade

É a garantia de que a informação não estará disponível por pessoas, entidades ou processos não autorizadas. É o resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada.

3.1.2 Integridade

Enfatiza que as informações devem ser mantidas conforme emitidas por seu titular, garantindo sua proteção contra intencionalidade, impropriedade ou acidentes. Em outras palavras,

(61) 3035-3900
www.uniceplac.edu.br
Área Especial para Indústria
Lote nº 02, Bloco A, Sala 304,
Setor Leste, Gama, Brasília, DF
CEP 72.445-020

é uma garantia de que a informação armazenada é o que será recuperado.

3.1.3 Disponibilidade

É uma garantia de que as informações devem estar disponíveis sempre que seus usuários (pessoas e empresas autorizadas) precisarem dela. Propõe que tudo seja feito de maneira eficiente, rápida e sem impactos negativos na atividade, ou seja, o acesso precisa ser fácil, os processos precisam ser eficientes e os sistemas devem funcionar de maneira veloz, sem travar.

4 PROCEDIMENTOS E ANÁLISE DOS DADOS

Com o número crescente de dispositivos IoT, a segurança está se tornando uma prioridade. Empresas como Intel, Samsung e Google estão se dedicando cada vez mais para proteger os dispositivos de borda, conexão do IoT com as empresas, com recursos de segurança.

A Intel oferece recursos básicos de segurança para ajudar a proteger aplicações de IoT, investindo em quatro categorias de segurança fundamentais, uma delas é a integridade da plataforma que mitiga a adulteração, aproveitando a raiz de hardware da proteção baseada na confiança de firmware, código e dados críticos da plataforma. A proteção aprimorada para dados, chaves e ID oferece opções integradas e discretas para credenciais resistentes à adulteração. Também oferece aceleração de criptografia e geração de chaves seguras para maior eficiência e desempenho geral e uma execução confiável que estabelece uma proteção baseada em hardware para ambientes de execução de aplicativos ou cargas de trabalho com recursos compartilhados.

O *Google Cloud Internet of Things* (IoT) *Core* é um serviço totalmente gerenciado para conectar e gerenciar dispositivos IoT com segurança. Para proteger os serviços IoT contra ameaças e fraudes, o Google possui o *Cloud Armor* que protege suas aplicações contra os *distributed-Denial-of-Service* (DDoS), ataques de rede distribuídos, filtra as solicitações recebidas da Web por região geográfica ou um host de parâmetros, como cabeçalhos de solicitação, cookies ou strings de

(61) 3035-3900
www.uniceplac.edu.br
Área Especial para Indústria
Lote nº 02, Bloco A, Sala 304,
Setor Leste, Gama, Brasília, DF
CEP 72.445-020

consulta. O Cloud Armor também é um firewall de aplicativos da Web (WAF, na sigla em inglês) completo e contém regras pré-configuradas do conjunto de regras principais do *ModSecurity* para evitar ataques mais comuns na Web e as tentativas de exploração de vulnerabilidade.

Também usa o Apigee, que incorpora segurança às APIs em questão de minutos. Com as políticas prontas para uso, os desenvolvedores podem aumentar as APIs com recursos para controlar o tráfego, melhorar o desempenho e reforçar a segurança. O Apigee fornece um modelo de segurança positivo que compreende a estrutura das solicitações da API para que possa distinguir com mais precisão o tráfego válido e o inválido.

A Samsung conta com o *Samsung Knox Manage* (combinação de base de segurança integrada aos dispositivos Samsung, criando um conjunto completo de soluções empresariais que utilizam a plataforma *Secured by Knox*). Conforme a tabela 2 podemos notar os meios para referência de recursos de segurança.

Tabela 2 – Recursos de segurança de Samsung Knox

Recursos	**Descrição**
Remote Device Health	Obtenha visibilidade de quais dispositivos têm problemas de segurança, como firmware não autorizado, permitindo que você aja imediatamente. Knox verifica o registro de adulteração de IMEI e se a garantia foi danificada.
Knox Vault	Um subsistema isolado, à prova de adulteração e seguro com seu próprio processador e memória, o Knox Vault armazena dados confidenciais, como chaves do Android Keystore suportadas por hardware, a chave de atestado Samsung, dados biométricos e credenciais de blockchain. Ele executa um código crítico de segurança que autentica os usuários com tempos limite crescentes entre falhas e controla o acesso às chaves, dependendo da autenticação.
Keystore Support of eSE & Other High-Security Storage	Vários serviços exigem credenciais para acesso. Eles incluem Wi-Fi, VPN, e-mail e sites. Para armazenar credenciais confidenciais com segurança, os desenvolvedores precisam escrever um novo código de armazenamento de credencial para qualquer novo hardware de armazenamento. A Knox fornece uma estrutura plug-and-play para gerenciamento de credenciais em uma variedade de hardware, eliminando a necessidade de desenvolver uma lógica de implementação de gerenciamento de credencial interna.
Sensitive Data Protection (SDP)	O SDP mantém os dados criptografados enquanto um perfil de trabalho ou dispositivo totalmente gerenciado está bloqueado, mesmo durante o tempo de execução quando outras soluções descriptografam dados.
Real-Time Kernel Protection (RKP)	Limita drasticamente os possíveis ataques a dispositivos Samsung com os melhores recursos de prevenção de ataques de kernel: Kernel Text Protection (KTP): protege contra qualquer tentativa de falsificar ou manipular o texto do Kernel (código e dados RO).

(61) 3035-3900
www.uniceplac.edu.br
Área Especial para Indústria
Lote nº 02, Bloco A, Sala 304,
Setor Leste, Gama, Brasília, DF
CEP 72.445-020

	Proteção de Tabela de Página (PTP): Protege contra qualquer tentativa de forjar ou manipular o Kernel e a tabela de página do usuário.
	Kernel Data Protection (KDP): Protege contra qualquer tentativa de forjar ou manipular o namespace / credencial / ID de segurança / mapa duplo do kernel, incluindo código do kernel, dados do kernel e proteções de fluxo de controle do kernel.
	Proteção de Fluxo de Controle (CFP): impede ataques de Programação Orientada a Retorno (ROP) e Programação Orientada a Saltos (JOP) que reutilizam a lógica do kernel existente para reunir exploits do próprio código do kernel.
DualDAR Encryption	Com uma única instância de criptografia, possíveis falhas na implementação podem resultar em um único ponto de falha. KPE DualDAR fornece duas camadas independentes de criptografia para atingir um nível ainda mais alto de confiabilidade, permitindo redundâncias na proteção de dados em repouso. Você pode fortalecer ainda mais a criptografia de dados usando um módulo criptográfico de terceiros para personalizar a criptografia.
	Essa criptografia dupla é necessária para implantações classificadas. Observe que há uma taxa de licença adicional para usar DualDAR.
ML Model Protection	Modelos de aprendizado de máquina e neural vêm com desafios de segurança exclusivos que são difíceis de resolver.
	sem suporte da plataforma de sistema operacional móvel. O Knox ML Model Protection aproveita a plataforma Knox para fornecer aos desenvolvedores criptografia segura, operação e controle de acesso dos modelos de ML.
Enforced Two-Factor Authentication	Permite que os administradores de TI forcem a autenticação de dois fatores do usuário final para fazer login em um perfil de trabalho ou dispositivo totalmente gerenciado. A autenticação de dois fatores é feita por meio de uma combinação de biometria (impressão digital, íris, rosto) e meios mais tradicionais (senha, PIN, padrão).
Government-Grade Common	Simplifica a configuração de dispositivos em um estado compatível para implantações de Critérios Comuns (segurança nacional).
Criteria Mode	
Separated Apps	Para empresas que precisam de controle total sobre um dispositivo corporativo, ao mesmo tempo em que habilita terceiros autorizados
	aplicativos de negócios de terceiros, a Samsung oferece aplicativos separados exclusivamente para isolar aplicativos de terceiros em uma pasta em sandbox.
App Isolation Groups (SEAMS)	Ao contrário dos contêineres de aplicativos clássicos com uma GUI, você pode gerenciar grupos de isolamento de aplicativos "invisíveis" para proteger um conjunto de aplicativos de qualquer outro conjunto. São possíveis até 300 agrupamentos.
Secure Certificate Enrollment Agents (SCEP, CMP, CMC_EST protocols)	A Samsung fornece um conjunto gratuito de agentes de registro de certificados que seguem os protocolos de segurança mais recentes. Não há razão para inscrever certificados de forma insegura ou implementar seus próprios protocolos.

Fonte: Samsung Knox Platform for Enterprise - White Paper, jul/2021.

(61) 3035-3900
www.uniceplac.edu.br
Área Especial para Indústria
Lote nº 02, Bloco A, Sala 304,
Setor Leste, Gama, Brasília, DF
CEP 72.445-020

5 CONSIDERAÇÕES FINAIS

A Internet das coisas foi um enorme avanço tecnológico e inovador. Segundo Mathieu Le Roux**,** Cofundador da escola de programação Le Wagon Brasil, "todas as pessoas precisarão se reinventar várias vezes na vida para lidar com as mudanças impostas pelo avanço tecnológico". Seu funcionamento possui grande relevância e melhoria para qualidade de vida das pessoas e corporações. É de suma importância o papel da segurança da informação, como garantia para os benefícios que sua efetiva aplicação oferece aos usuários. As políticas de segurança devem ser respeitadas, pois o alto risco de vulnerabilidade existentes nos dispositivos IoT deixam fragilizados os dados pessoais, para possíveis ataques cibernéticos.

Os avanços tecnológicos são inquestionáveis, cada vez mais presente no dia a dia, modificando o comportamento das pessoas, o modo de fazer compras, interagir, fazer amizades, ver filmes, ler notícias e principalmente a forma de se informar. Mensurada pela segurança da informação, foram analisadas as vantagens e desvantagens sobre a Internet das Coisas, onde busca-se uma reflexão referente à vulnerabilidade e aos critérios de segurança na IoT. Deste modo, se cada vez mais dispositivos eletrônicos fizerem parte do nosso dia a dia, é importante discutir se a tecnologia automatizada e em rede, que complexifica as discussões sobre gerência, autoria, propriedade e privacidade das informações, oferece a segurança necessária.

Ao comparar empresas como Intel, Samsung e Google, verificamos que os dispositivos inteligentes disponíveis para automação residencial possuem interfaces individuais de controle, bem diferentes entre si, tornando o processo de controle de um ambiente multidispositivos mais difícil para o usuário, além disso torna mais complicado o processo de manter a segurança de todo o ambiente sob controle. Portanto a adoção de protocolos de segurança mais rígidos é um dos principais métodos contra ataques e invasões gerais.

(61) 3035-3900
www.uniceplac.edu.br
Área Especial para Indústria
Lote nº 02, Bloco A, Sala 304,
Setor Leste, Gama, Brasília, DF
CEP 72.445-020

6 REFERÊNCIAS

ALVES, Gustavo Alberto. Segurança da Informação: uma visão inovadora da gestão. Rio de Janeiro: Ciência Moderna Ltda, 2006.

ATAQUES CIBERNÉTICOS. Fabiana Rolfini. Disponível em: https://olhardigital.com.br/2020/05/07/noticias/brasil-teve-mais-de-1-6-bilhao-de-ataques-ciberneticos-em-tres-meses/

BASSI, **Alessandro. Enabling Things to talk:** Designing IoT solutions with the IoT Architectural Reference model. New York, London. ed. Springer Open, 2013.

Brynjolfsson, Erik e McAfee, Andrew. The Second Machine Age: Work, Progress and Prosperity in a Time of Brilliant Technologies. New York, USA: editora W. W. Norton & Company, 2014.

GOOGLE, Cloud. Proteja sua organização com as soluções de segurança do Google Cloud. Disponível em: https://cloud.google.com/solutions/security/. Acesso em: 30 nov. 2021.

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

ISP. Ponto. Pesquisa da SonicWall mostra o crescimento de ataques a IoT. **PontoISP,** 2020. Disponível em: https://www.sonicwall.com/pt-br/lp/capture-labs/. Acesso em: 14 jun. 2021.

(61) 3035-3900
www.uniceplac.edu.br
Área Especial para Indústria
Lote nº 02, Bloco A, Sala 304,
Setor Leste, Gama, Brasília, DF
CEP 72.445-020

MARKETING. Revista Live. Ataques cibernéticos crescem 300% durante a pandemia. **ADNEWS**, 2021. Disponível em: https://revistalivemarketing.com.br/ataques-ciberneticos-crescem-300-durante-a-pandemia/. Acesso em: 15 jun. 2021.

PUC, Minas. Segurança da informação. Disponível em: https://www.pucminas.br/si/Paginas/default/. Acesso em: 30 nov, 2021.

VENTURELLI, Marcio. Protocolos de IoT. Educação, automação industrial e transformação digital**,** 2020. Disponível em: https://marcioventurelli.com/2020/07/23/protocolos-de-iot-internet-das-coisas-mqtt/

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

SPARROW. Gold. A NASA Informa um Aumento nos Ataques de Malware Enquanto o Seu Pessoal Trabalha em Casa. **EnigmaSoft**, 2020. Disponível em: https://www.enigmasoftware.com/pt/nasa-relata-aumento-ataques-malware-enquanto-pessoal-trabalha-casa/. Acesso em: 14 jun. 2021.

WAHER, Peter. Learning Internet of Things. Birmingham, UK: editora Packt Publishing.

(61) 3035-3900
www.uniceplac.edu.br
Área Especial para Indústria
Lote nº 02, Bloco A, Sala 304,
Setor Leste, Gama, Brasília, DF
CEP 72.445-020