**Política de Segurança da Informação de baixo custo para empresas de pequeno e médio porte**

**Igor da Silva Zagonel1**

1IFMT - Campus Cuiabá - Cel. Octayde Jorge da Silva, Departamento de Computação

igorzagonel@gmail.com

***Resumo.*** *A necessidade de utilizar sistemas de informação no meio empresarial para aumentar a produtividade e conseguir vantagem em relação a concorrência vem sendo amplamente difundido no mercado de trabalho o que levou a um aumento de crimes relacionados à segurança da informação que são prejudiciais ao funcionamento da empresa e no lucro obtido por ela. Por causa de tamanha importância os equipamentos necessários para realizar a segurança da parte computacional da empresa são extremamente custosos, o que influencia empresas de pequeno e médio porte a não adotarem esses sistemas, mesmo elas sendo tão vulneráveis quanto grandes empresas. Assim, o objetivo deste trabalho é desenvolver uma proposta de uma política de segurança de baixo custo para empresas de pequeno e médio porte. A partir do levantamento de conceitos utilizando as ferramentas de busca Google Acadêmico, BDTD e o Portal de Periódicos da CAPES foi possível escolher a composição de softwares e hardwares para a proposta. Nota-se que a proposta construída usa apenas softwares gratuitos e hardwares com preços extremamente acessíveis até mesmo para empresas pequenas.*

# 1. Introdução

Devido ao crescente avanço tecnológico nos sistemas de informação e do armazenamento de dados, houve como resultado a redução do tempo gasto para realizar consultas e utilizar as informações, em virtude dessa vantagem muitas empresas atualizam suas tecnologias para aumentar sua produtividade (CAMPOS-FILHO, 1994).

Na segurança da informação há alguns termos que são muito utilizados para se referenciar a certos acontecimentos, sendo esses termos (SÊMOLA, 2003):

1. Ativo: É todo recurso que pode sofrer algum tipo de dano, sendo assim tendo a necessidade de ser protegido.
2. Vulnerabilidades: São fraquezas que existem em um sistema de segurança que podem ser exploradas por pessoas com intenções maliciosas a fim de obter algum tipo de vantagem ou até mesmo destruir algum ativo.
3. Ameaça: É algo que oferece risco a um ativo e possivelmente explora uma vulnerabilidade para conseguir danificar o mesmo.
4. Ataque: É o evento que ocorre ao se explorar uma vulnerabilidade a fim de causar algum mal para o ativo em questão.
5. Incidente: É um conjunto de eventos que decorrem a partir de um ataque que explora uma vulnerabilidade que leva à perda dos princípios básicos da segurança da informação.

Dessa maneira as empresas são expostas a novos riscos e vulnerabilidades, pois a segurança computacional trata-se de um processo vivo, enquanto alguns estão criando novas metodologias de segurança e obstáculos que dificultem o acesso aos dados sigilosos, outros estão estudando como burlar ou quebrar a metodologia ou modelo recém-criado (FERNANDES, 2000). Logo, é extremamente difícil construir um sistema de segurança da informação a prova de falhas, mas é possível minimizá-las a um nível aceitável.

A fim de minimizar essas falhas é necessário a existência de uma política de segurança da informação que consiste em um documento que é baseado nos requisitos de segurança necessários da empresa e é redigido a partir de uma análise profunda de todos os fundamentos da empresa para que seja possível obter a melhor eficiência e proteção possível (ASSAD, 2002). Dentre as falhas e brechas possíveis na segurança da informação de uma empresa o autor Joel Witts (2021) descreve 5 das principais ameaças à segurança de uma empresa pequena, elas são respectivamente: ataques de phishing, ataques de malwares, ransomware, senhas fracas e ataques internos.

Partindo dessas falhas é possível encontrar algumas soluções para evitar as suas ocorrências. Em relação aos ataques de phishing e as senhas fracas um bom treinamento contra engenharia social é necessário, pois ambas as brechas fazem uso dessa técnica chamada engenharia social, esse método consiste de diversas maneiras de obter informações relevantes a partir de uma pessoa, nesse sentido os ataques de phishing baseiam-se em personificar identidades que tem a confiança da empresa ou do indivíduo com a finalidade de conseguir uma brecha na segurança através de um link ou um arquivo malicioso (WITTS, 2021; SILVA; ARAUJO; AZEVEDO, 2013).

Da mesma maneira que o ataque de phishing utiliza o próprio psicológico da pessoa para obter vantagens, a previsão das senhas usadas por esse indivíduo pode ocorrer utilizando essas técnicas de engenharia social dependendo de como essa senha é formada, um exemplo de uma senha com alta probabilidade de ser comprometida é utilizar a data de aniversário de um ente querido como uma senha, ao fazer uso desse tipo de senha, a probabilidade dela ser descoberta por terceiros é extremamente alta devido a facilidade de se conseguir esse tipo de informação em redes sociais ou até mesmo conversas informais (WITTS, 2021).

Além das vulnerabilidades geradas por atos maliciosos utilizando engenharia social existem também as falhas técnicas que podem levar a perdas enormes. No que se diz respeito às principais ameaças técnicas estão os ataques de malwares e os ransomware que exigem diversos cuidados a serem tomados pela empresa ou indivíduo para evitar danos desses métodos. Assim sendo, os malwares podem ser definidos como softwares maliciosos que são usados para invadir e adquirir informações ou destruir dados de computadores de terceiros. O ransomware é essencialmente um malware, o que muda é a abordagem de como é realizado esse tipo de ataque, ele consiste em sequestrar os dados de uma organização encriptando-os com uma criptografia avançada de modo que seja praticamente impossível quebrá-la e após o sucesso desse sequestro é pedido um resgate em dinheiro para liberar esses dados novamente, o que leva a empresa em um dilema, perder uma grande quantidade de dinheiro e recuperar os dados ou perder todos os dados presentes nos computadores (CERT.BR 2012).

Para evitar esses acontecimentos a organização deve implementar certas medidas para evitar essas ameaças, entre essas medidas as mais importantes são o antivírus e o firewall, assim sendo o firewall pode ser considerado como como uma combinação de software e hardware que separa a rede interna da organização da internet em geral, o que torna possível o administrador controlar certos aspectos da rede, já o antivírus pode ser considerado uma ferramenta antimalware que é desenvolvida com o intuito de eliminar possíveis ameaças e brechas de segurança de um computador. Consequentemente esses softwares têm extrema influência no confronto de ameaças como os malwares e os ransomware além de estarem intrinsecamente ligados ao nível de segurança da informação de uma empresa (CERT.BR, 2012; KUROSE, 2013).

(Ver com a professora se eu coloco a parte de segurança física aqui ou já está muito carregado a introdução)

         Em consequência dessas ameaças aos sistemas computacionais, toda empresa que utiliza esses meios está sujeita ao mesmo risco de segurança independentemente do sistema utilizado por ela, porém as pequenas e médias empresas são severamente afetadas pelos problemas de adotar novas tecnologias porque não possuem um grande capital para investir em um sistema de qualidade, diferentemente das grandes empresas que podem adquirir um sistema de segurança da informação de alto nível pagando preços exorbitantes sem afetar o financeiro da empresa.

         Sendo assim, este artigo tem como objetivo elaborar um modelo de política de segurança da informação utilizando softwares gratuitos e hardwares com preços acessíveis para diminuir os custos e cobrir boa parte das principais vulnerabilidades de empresas de pequeno e médio porte.

         Para tanto, este artigo está estruturado, além desta primeira seção de introdução em mais quatro seções. Na seção 2, se encontram os materiais e métodos utilizados na pesquisa. Na seção 3, são apresentados os principais conceitos de segurança da informação. Na seção 4 é apresentado o modelo de segurança proposto por este artigo. Na seção 5, são realizadas as conclusões e discussões sobre a proposta sugerida.

# 2. Materiais e Métodos

(Insira materiais e métodos aqui)

# 3. Referencial Teórico

Esta seção consiste em revisar trabalhos existentes sobre segurança da informação, a fim de fundamentar todo o estudo baseando-se em artigos, monografias, teses e livros.

# 3.1 Segurança da informação

Com o passar do tempo, o uso generalizado de equipamentos para processar e armazenar informações sofreu uma modernização exponencial, com toda essa evolução os modos de armazenamento antigos, como armários gigantescos ou salas com diversos arquivos impressos se tornaram obsoletos e ineficientes. Esse desenvolvimento global é consequência da introdução do computador na vida das pessoas e das organizações, porém com a chegada dessa tecnologia novos perigos foram criados e com esses riscos a necessidade da segurança da informação se tornou essencial para criar métodos e ferramentas para proteger as informações. É possível separar o escopo de segurança da informação em uma organização em duas partes, uma delas sendo a segurança de computadores que é o conjunto de ferramentas criados para proteger dados devido a presença marcante dos computadores nas vidas das pessoas e a segunda sendo a segurança de inter-rede que é o grupamento de ferramentas encarregadas de proteger os dados durante a transmissão entre um emissor e um receptor por causa da introdução dos sistemas distribuídos e o uso de redes interligadas para o compartilhamento de informações (STALLINGS, 2008).

De acordo com Castro (2011, *apud* DIAS; RODRIGUES; PIRES, 2012), a segurança da informação se resume em métodos que protegem a integridade das informações de uma empresa, tanto no quesito computacional como nos ambientes externos e internos da instituição. A proteção dessas informações é fundamentada no uso de uma série de softwares e hardwares que oferecem controle dos principais processos da empresa a fim de serem monitorados, analisados e melhorados caso haja a necessidade, com isso é possível obter-se um sistema com um nível aceitável de segurança, desde que o sistema apresente um controle pleno das informações da organização (ISO/IEC 17799, 2005).

Segundo Stallings (2015), a partir da definição de que a segurança da informação é a proteção de um sistema informatizado e que essa proteção propõe-se em alcançar a preservação da integridade, da disponibilidade e da confiabilidade das informações do sistema. Fundamentando-se nessa declaração é possível extrair 3 objetivos principais que são o cerne da segurança de computadores sendo eles a confidencialidade que é a segurança de que informações sigilosas sejam acessadas somente por indivíduos previamente autorizados e além disso deve haver o controle por parte dos indivíduos sobre quais informações relacionadas a eles serão armazenadas ou reveladas, a integridade que assegura que as informações presentes no sistema computacional não sejam adulteradas de uma maneira não autorizada previamente e também o sistema em que essas informações estão armazenadas deve funcionar de maneira livre e ilesa de manipulações não autorizadas de qualquer tipo e por fim a disponibilidade que consiste que as informações presentes no sistema estejam sempre disponíveis para aqueles que têm a autorização para acessar esses dados (STALLINGS, 2015).

Além das definições convencionais de confiabilidade, integridade e disponibilidade, é possível definir também outros dois traços importantes que são a autenticidade e o não-repúdio. A autenticidade baseia-se na segurança de que quem receba a informação seja quem ele afirma ser, ou seja, não ser um impostor assumindo a identidade de uma pessoa conhecida para conseguir informações e o não-repúdio fundamenta-se na certeza que o receptor/emissor de uma informação não possa negar que tenha emitido ou recebido a mensagem. Ao analisar o conceito de autenticidade percebe-se que ela é um pré-requisito para as definições convencionais, pois sem a autenticação devidamente feita não é possível saber se uma modificação ou acesso foi devidamente autorizado e o não-repúdio que normalmente aparece em serviços de comunicação tem como função assegurar a origem de quem enviou aquela informação (LANDWEHR, 2001).

Partindo dessas definições comuns, Stallings (2015) descreve alguns dos principais desafios na implantação da segurança de computadores sendo eles:

1. Mesmo com aspectos relativamente simples a segurança da informação pode ser complicada para um iniciante, pois os requisitos podem ser claros e auto explicativos baseando-se na confidencialidade, autenticação, não-repúdio ou integridade, porém os mecanismos utilizados para satisfazer esses requisitos podem ser complexos e nebulosos para o entendimento.
2. Ao desenvolver um algoritmo ou mecanismo de segurança é necessário sempre considerar potenciais ataques e brechas dessas funcionalidades, porém a grande maioria dos ataques bem sucedidos são projetados partindo de um ponto de vista completamente diferente do mecanismo criado, explorando assim uma fraqueza inesperada.
3. Por conta do ponto acima os procedimentos de segurança não são intuitivos uma vez que esses mecanismos são extremamente complexos dado que são levadas em consideração diversos aspectos que podem se tornar uma ameaça no futuro.
4. Os procedimentos de segurança criados vão além de apenas algoritmos ou algum protocolo de comunicação. Eles requerem muitas vezes que os indivíduos envolvidos possuam certas informações secretas (como senhas ou chaves de encriptação), o que leva a outros problemas relacionados à criação, armazenamento e distribuição dessas informações, além de adversidades por causa de outras influências externas do mecanismo de segurança criado, como por exemplo, se uma ferramenta de segurança precisa para funcionar plenamente limitar o tempo de trânsito de uma mensagem entre um emissor e um destinatário se acaso o meio de comunicação tiver atrasos imprevistos a ferramenta de segurança pode perder o sentido de existência.
5. A segurança de computadores é basicamente uma batalha entre um atacante e um defensor, sendo o atacante um hacker com intenções maliciosas tentando achar brechas para invadir um sistema e o defensor sendo o administrador de uma rede esforçando-se para prevenir todas as possíveis brechas o que o deixa em clara desvantagem, pois o atacante deve achar somente uma brecha e seu trabalho está concluído, já o administrador deve se preocupar com todas as falhas possíveis.
6. Existe a tendência dos indivíduos ignorarem as vantagens de se ter um sistema de segurança bem desenvolvido até o momento que uma falha ocorra.
7. A segurança sempre requer um monitoramento regular, o que é difícil de conciliar com os ambientes sobrecarregados de hoje em dia devido ao tempo e esforço gasto nessa atividade.
8. A segurança normalmente não é desenvolvida no processo de criação de um sistema e sim acrescentada na finalização do planejamento, o que leva a possíveis falhas.
9. Muitos usuários e administradores vêem a segurança como um impedimento para um processo mais rápido e eficiente.

         Essas vulnerabilidades e desafios da segurança da informação estão intrinsecamente ligadas ao erro do procedimento de segurança criado, o que resulta em uma informação não confiável (LYRA, 2015). Sendo assim, conforme as facilidades tecnológicas se expandem as empresas tendem a se tornarem dependentes dessas tecnologias, o que leva a vulnerabilidades que ocasionam crimes e fraudes de informações utilizando meios computacionais (CARUSO; STEFFEN, 1999 *apud* SILVA-NETTO; SILVEIRA, 2007).

Portanto, para garantir a confiabilidade, a disponibilidade e a integridade das informações da organização é necessário que seus gestores tenham conhecimento das possíveis ameaças, com o objetivo de apresentar uma solução específica para cada problema encontrado, pois a maioria dos dados de uma grande empresa estão contidos em seus sistemas computacionais e por isso é necessário que a integridade do dado esteja intacta a fim de evitar consequências graves para o funcionamento da empresa (SILVA-NETTO; SILVEIRA, 2007).

# 3.2 Políticas de Segurança

A definição e implantação de políticas de segurança da informação em uma empresa vem ganhando muita importância com a evolução dos sistemas de informação, gerando assim diversos desconfortos em relação às responsabilidades e os deveres de cada membro dentro de uma empresa, isso se deve ao fato de que uma política de segurança deve abranger todos os aspectos de uma organização, desde os mais simples como implicações físicas de quem vai poder acessar uma certa sala até mesmo em âmbito jurídico em relação às punições de quem infringir essa política criada. Logo, uma política de segurança necessita de alguns pontos básicos imprescindíveis para sua construção, sendo eles (ASSAD,2002):

1. Ter uma introdução que abranja todos os objetivos e definições necessárias para o entendimento de todos em uma organização.
2. Mecanismos de suporte às políticas de segurança.
3. Uma explicação de cada política de segurança adotada e suas influências e relevâncias dentro da organização.
4. A definição das responsabilidades gerais dos indivíduos envolvidos no escopo da política de segurança, isso é, definir as obrigações o mais especificamente para os diferentes setores e pessoas que estarão incluídas.
5. Sempre ter a referência de outros documentos para dar embasamento para a política de segurança adotada.

Sendo assim, a política de segurança da informação utilizada em uma empresa pode ser definida como um documento que contém os valores, as responsabilidades e os requisitos necessários que a empresa e o sistema de segurança da informação devem cumprir a fim de manter a integridade das informações (DANTAS, 2011).

Consequentemente, para começar um sistema de segurança da informação que atenda a todos os requisitos necessários de proteção é preciso respeitar os controles essenciais da empresa definidos pela ISO/IEC 17799 (2005) como sendo: proteger dados e informações pessoais, proteger registros organizacionais e ter direito sobre a propriedade intelectual. Tendo em vista o controle exercido pela empresa sobre suas informações, é essencial que a empresa identifique os requisitos de segurança que são necessários para o seu funcionamento, existem três fontes de levantamento de requisitos de segurança da informação, sendo elas:

1. É obtido através de uma análise dos possíveis riscos e brechas de segurança que a empresa pode sofrer, levando em conta todo o planejamento estratégico da organização para que não haja brechas e vulnerabilidades;
2. Pode ser obtida a partir da legislação que oferece regulamentos que demonstram as obrigações legais da empresa;
3. É desenvolvida a partir dos requisitos de processamento de dados que a empresa necessita para seu funcionamento.

O resultado de toda essa preparação e levantamento de dados para desenvolver a política de segurança resulta nas direções gerais para os indivíduos da organização seguirem e também as ferramentas necessárias para dar suporte a esse novo regulamento (ISO/IEC 17799, 2005).

As políticas de segurança da informação criadas devem também ser implementadas de forma realista e flexível levando em consideração a realidade da organização além de ter as  definições explícitas e precisas das responsabilidades de cada indivíduo envolvido na gestão desse sistema. No documento gerado os aspectos técnicos de implementação das medidas de segurança devem ser deixados de lado, pois essas implementações podem mudar ao longo do tempo devido a mudança do alinhamento estratégico da empresa, além de que o documento da política de segurança de uma empresa deve ser de fácil leitura para todos as pessoas envolvidas possam entender com clareza seu significado, desde os indivíduos com mais instrução acadêmica até os indivíduos com pouca instrução (LYRA; TORMIM; NISHI, 2014).

Como retratado anteriormente, uma política de segurança da informação é construída a partir de uma análise profunda de todos os requisitos de segurança da empresa, assim sendo, as políticas de segurança de empresas distintas podem ter inúmeros pontos em comum e serem baseadas nas mesmas normativas, mas é extremamente difícil elas serem iguais, pois podem diferenciar-se nos hardwares e softwares utilizados para a constituição do sistema de segurança da informação. Em vista disso, o estabelecimento de uma nova política de segurança em uma empresa normalmente é um processo longo e demorado, pois é necessário mudar rotinas consideradas corretas para novas práticas que levam em consideração a segurança e integridade da empresa (ASSAD, 2002).

# 3.3 Camadas da Segurança da Informação

Para a existência de um sistema de segurança da informação é necessário um conjunto elementar de componentes interligados que coleta, manipula e processa dados e informações essenciais para o funcionamento de uma organização, esse conjunto de componentes é composto por hardware, software, pessoas e processos que são a base da infraestrutura de segurança de uma empresa (DANTAS, 2011).

A partir desses componentes essenciais Sêmola (2003, *apud* SILVA-NETTO; SILVEIRA, 2007, p.379) define a gestão de segurança da informação em 3 aspectos principais: software, hardware, humano; e Adachi (2004) define a gestão de segurança da informação em três camadas distintas, sendo elas: física, lógica e humana. Logo, é necessário um equilíbrio entre esses aspectos para que não haja vulnerabilidades, pois é muito comum as empresas focarem apenas em softwares como firewalls, antivírus, e não dar importância para os demais componentes.

Desta maneira, a figura 1 demonstra de forma visual os domínios referentes a cada camada:



**Figura 1. Classificação dos domínios referentes a cada camada (ADACHI, 2004).**

 1º - Camada Física: Ela é composta pelo ambiente onde os equipamentos e periféricos estão instalados, sendo eles computadores, servidores ou qualquer hardware interligado com o sistema, uma das formas para conduzir a segurança desta camada é o controle de acesso através de senhas ou leituras biométricas (ADACHI, 2004). A partir da forma de gerir a segurança da camada física é possível reconhecer o erro da maioria das empresas de pequeno e médio porte, pois estas empresas geralmente possuem dados em servidores locais que possuem conexão com a internet, o que aumenta o risco de invasão, e elas não se preocupam em restringir o acesso à apenas os funcionários responsáveis pela rede da organização (SILVA-NETTO; SILVEIRA, 2007).

2º - Camada Lógica: Esta camada é composta por todo software utilizado na empresa, ou seja, os softwares são os responsáveis por coordenar e gerenciar as informações da organização a fim de realizar uma ação em específico e também é nessa camada onde estão as regras e normas de comunicação que ficam ocultas ao usuário (ADACHI, 2004). Sendo assim, a segurança em nível lógico pode ser entendida como o acesso que os indivíduos têm a aplicações ambientadas em sistemas informatizados e as ferramentas de controle de informação podem ser compreendidas como entidades "invisíveis" na sua maior parte para os usuários de um sistema informatizado e que normalmente só é revelado sua existência a usuários externos do ambiente de informática quando ocorre uma barramento de acesso a uma informação (CARUSO; STEFFEN, 1999). Logo, para prevenir brechas de segurança é importante que se mantenha atualizado todos os softwares utilizados na empresa, a fim de minimizar os riscos (SILVA-NETTO; SILVEIRA, 2007).

3º - Camada Humana: Ela é formada por todo recurso e mão de obra humana que está presente no ambiente de trabalho, principalmente aqueles que têm acesso aos recursos computacionais da empresa, dentre os incidentes de segurança que ocorrem estão a falta de instrução dos usuários no uso da TI (tecnologia da informação), funcionários maliciosos ou ingênuos e a engenharia social (ADACHI, 2004). Segundo Schneier (2001) a camada humana é o elo mais frágil de toda a estrutura de gerenciamento de segurança da informação, sendo a responsável pela falha da corrente da segurança de muitos sistemas. Sendo assim, para uma gestão de segurança da informação eficiente é necessário atentar-se ao gerenciamento e supervisão de pessoas, pois muitas empresas se descuidam em relação a este fator (SILVA-NETTO; SILVEIRA, 2007).

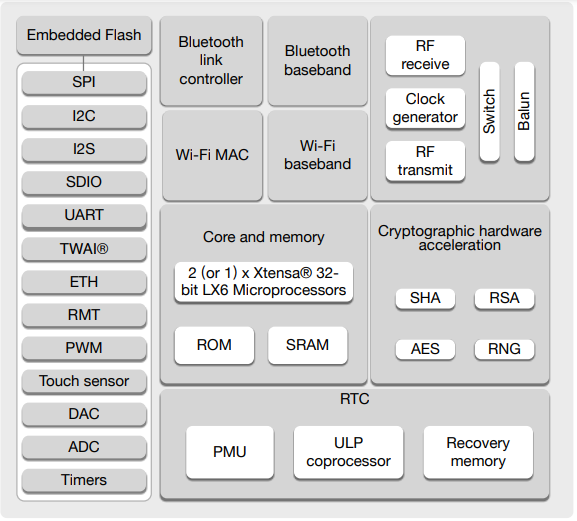
# 3.2 Microcontrolador ESP32

Com o atual estágio de desenvolvimento da microeletrônica é possível adaptar e traduzir diversos problemas complexos da realidade utilizando componentes eletrônicos em conjunto com microprocessadores para resolver as mais diversas dificuldades que enfrentamos no dia a dia. Em vista disso, ao pensar-se em desenvolver um sistema inteligente, além dos componentes eletrônicos e sensores necessários para realizar as ações requeridas, o microcontrolador é a peça fundamental para qualquer sistema, pois são os responsáveis por gerenciar e controlar todo o sistema criado e muitas vezes tambem é o incubido de transmitir essas informações para algum lugar (DIAS; 2021). Sendo assim, é possível definir um microcontrolador como um equipamento programável de baixo custo que faz a integração em uma placa pequena de diversos componentes como a unidade de processamento, memórias, entradas e saidas, controle temporal, conversores analogicos e digitais entre outros diversos elementos que podem fazer parte dependendo do modelo do microcontrolador analisado (SANTOS;LARA, 2019).

O microcontrolador ESP 32 é um avançado microcontrolador desenvolvido pela renomada empresa Espressif Systems que possui sua sede em Xangai. Esse equipamento foi apresentado ao público em 2016 e desde então vem sendo empregado em diversos projetos de sistemas inteligentes devido a sua robustez e a incrível quantidade de funcionalidades implementadas em um chip que cabe na palma da mão (DIAS; 2021).

Dentre as funcionalidades que destacam o ESP 32 de seus outros concorrentes está a sua incrível quantidade de memória flash para armazenamento e a velocidade de processamento que pode chegar  até 240 MHz dependendo de como está configurado, além dessas características de processamento e armazenamento de dados o ESP 32 possui dois tipos de comunicação sem fio integradas na placa, sendo elas o Wi-fi e o bluetooth. Com base nisso, é possível entender o motivo desse microcontrolador ser tão utilizado em sistemas inteligentes, pois além de possuir todos os módulos necessários para se conectar com a internet e enviar informações ele ainda possui uma otimização para consumir pouca energia enquanto funciona (SANTOS;LARA, 2019).

Além desses componentes já descritos o ESP 32 conta com diversas outras características que facilitam no desenvolvimento de sistemas inteligentes como demonstrado no diagrama de bloco da figura 2:



**Figura 2. Diagrama de blocos funcional (ESPRESSIF, 2021).**

Com base no diagrama da figura 2 é pode-se observar a enorme quantidade de elementos que o microcontrolador ESP 32 possui, ao olhar mais detalhadamente podemos constatar as seguintes especificidades (ESPRESSIF, 2021):

1. Memória e CPU (CPU and Memory):

* Xtensa® single-/dual-core 32-bit LX6 microprocessor(s)
* CoreMark® score:
* 1 core at 240 MHz: 504.85 CoreMark; 2.10 CoreMark/MHz
* 2 cores at 240 MHz: 994.26 CoreMark; 4.14 CoreMark/MHz
* 448 KB ROM
* 520 KB SRAM
* 16 KB SRAM in RTC
* QSPI supports multiple flash/SRAM chips

1. Relógios e Timers (Clocks and Timers):

* Oscilador interno de  8MHz com calibração
* Oscilador interno RC com calibração
* Cristal oscilador externo de 2 MHz ~ 60 MHz (40 MHz somente para funcionalidade Wi-Fi/Bluetooth)
* Cristal oscilador externo de 32 kHz para RTC com calibração
* Dois grupos de timer, incluindo timers de 2 × 64-bit e um 1 × watchdog principal em cada grupo
* Um timer RTC
* RTC watchdog

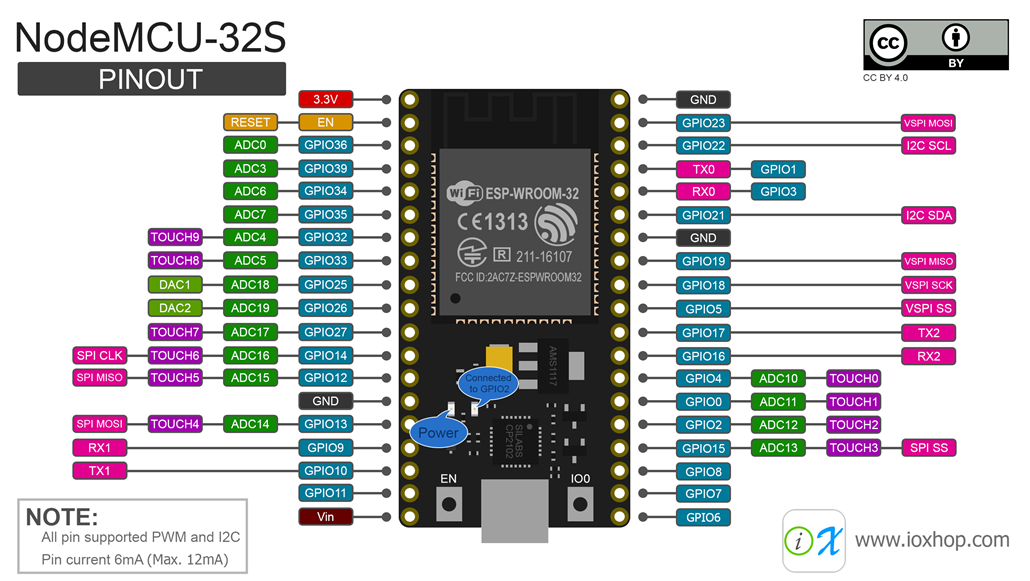
1. Interfaces periféricas avançadas (Advanced Peripheral Interfaces):

* 34 × pinos programáveis GPIOs
* 12-bit SAR ADC até 18 canais
* 2 × 8-bit DAC
* 10 × touch sensors
* 4 × SPI
* 2 × I2S
* 2 × I2C
* 3 × UART
* 1 host (SD/eMMC/SDIO)
* 1 slave (SDIO/SPI)
* Interface Ethernet MAC com DMA dedicado e suporte para IEEE
* TWAI®, compatível com ISO 11898-1 (CAN Specification 2.0)
* RMT (TX/RX)
* Motor PWM
* LED PWM até 16 canais
* Sensor hall

1. Segurança (Security):

* Boot seguro
* Criptografia de memória flash
* 1024-bit OTP, up to 768-bit for customers
* Aceleração de hardware criptografada.
* AES
* Hash (SHA-2)
* RSA
* ECC
* Random Number Generator (RNG)

Tomando como referência às características descritas a viabilidade do uso desse microcontrolador em diversos projetos é altíssima devido às suas características e sua construção como demonstrado na figura 3.



**Figura 3. Pinagem interna do ESP 32 (FERNANDO K., 2018).**

O módulo apresentado na figura 3 possui um regulador de tensão de 3,3V e possui também 36 pinos de entrada e saída para transmissão de dados (ESPRESSIF, 2021). Os pinos GPIO são os responsáveis por transmitir e receber diversos tipos de dados, sendo que o GPIO01 e o GPIO03 especificamente são responsáveis pelo tipo de comunicação RX/TX, os pinos a esquerda do microcontrolador realizam a atividade de converções analogicas para digitais, isto é, ele converte as informações captadas pelos sensores analogicos para sinais digitais para que o microcontrolador possa manipular e interpretá-las. Além desses recursos de comunicação e captação de informações o ESP 32 também possui recursos de economia de energia, ou seja, enquanto não for necessário o processamento de alguma informação o microcontrolador entra em um estado de repouso para economizar energia, e quando é necessário ele desperta desse estado e continua suas tarefas normalmente (ESPRESSIF, 2021; BORGES, 2019).

# 3.4 Internet das Coisas (IOT)

A internet das coisas (do inglês Internet Of Things(IOT)) emergiu do desenvolvimento de diversas áreas da tecnologia como os sistemas embarcados, microeletrônica, comunicação e o sensoriamento, assim sendo, a internet das coisas é um novo paradigma que emprega a união e conexão entre objetos físicos embarcados com diversos sensores e atuadores conectados através de uma rede sem fio que se comunicam por meio da internet. A partir do surgimento desse paradigma, uma quantidade imensa de possibilidades surgiu, pois com a interconexão da internet e desses objetos físicos que colhem dados do mundo real através de sensores é possível criar diversas aplicações que beneficiam dos novos tipos de dados e serviços que a IOT possibilita, por exemplo, ter um aplicativo de celular ou uma página web em que possa-se acionar um ar condicionado a partir de uma temperatura (PIRES;DELICATO;BATISTA;BARROS, Não sei).

A IOT pode ser considerada uma combinação de diversas tecnologias que viabilizam a integração de objetos e ambientes físicos com o ambiente computacional como foi retratado anteriormente e nesse sentido é possível definir blocos básicos que fazem parte da estrutura central da internet das coisas, sendo esses:

1. Identificação: É um dos blocos mais importantes devido a necessidade de identificar os objetos conectados na internet de maneira única e existem diversas tecnologias que tornam essa identificação possível, entre elas estão a tecnologia de Identificação Por Radio Frequencia (do inglês Radio Frequency Identification (RFID)) e o endereçamento IP.
2. Sensores/Atuadores: É o bloco que faz possível a coleta de informações do mundo real para o mundo digital, ou seja, os sensores coletam informações de onde os objetos físicos construídos estão e encaminham esses dados através de um meio de comunicação para um banco de dados e os atuadores podem interagir com o ambiente dependendo dos dados que foram adquiridos.
3. Comunicação: Esse bloco relaciona-se com as diversas técnicas que podem ser usadas pelos objetos inteligentes que usam IOT para comunicação de informações, além de que a comunicação tem uma responsabilidade crítica com o consumo de energia de um objeto IOT, entre as tecnologias que podem ser utilizadas para comunicação estão: WiFi, Bluetooth, IEEE 802.15.4.
4. Computação: Neste bloco estão contidas as unidades de processamento de dados que incluem os algoritmos aos objetos inteligentes, sendo elas, por exemplo, os microcontroladores e os processadores.
5. Serviços: A internet das coisas devido a sua alta gama de aplicabilidade a diversas situações provê diversos serviços diferentes e alguns deles se destacam na sua usabilidade, sendo eles:

* Serviços de identificação: Esses serviços são os responsáveis por mapear e transformar as entidades físicas em entidades virtuais, como por exemplo, transformar o valor lido por um sensor de temperatura em uma sala e transformá-lo em um valor em graus Celsius para mostrar em um aplicativo de celular.
* Serviços de agregação de dados: São os encarregados de coletar e sintetizar as informações obtidas dos objetos inteligentes que usam IOT.
* Serviços de colaboração e inteligência: Esses serviços agem sobre os serviços de agregação de dados utilizando as informações sintetizadas por eles para tomar decisões adequadas com as situações lidas.
* Serviços de Ubiquidade: São serviços que visam prover serviços de inteligência sempre que forem requisitados.

1. Semântica: Este bloco refere-se à habilidade de extração de informações e conhecimentos dos objetos dos objetos inteligentes que usam IOT, ou seja, trata-se de utilizar e gerir os conhecimentos e recursos adquiridos de forma eficiente partindo dos dados existentes, entre as técnicas que podem auxiliar na aplicação deste bloco estão: Resource Description Framework (RDF), Web Ontology Language (OWL) e Efficient XML Interchange (EXI).

Além desses blocos básicos que fazem parte da base da IOT, existe também uma arquitetura base para os objetos inteligentes construídos para serem utilizados com a internet das coisas, sendo essa arquitetura composta dos seguintes elementos:

1. Unidades de processamento e memória: Essa parte da arquitetura é composta por uma memória que é responsável por armazenar informações necessárias dentro do objeto inteligente, um microcontrolador o qual é incumbido de realizar a lógica necessária para o funcionamento desejado.
2. Unidades de comunicação: Consiste em no mínimo um canal que é responsável pela comunicação dos dados coletados que pode ser feita através de um fio ou utilizando outras tecnologias sem fio.
3. Fonte de energia: É o responsável por fornecer energia a todos os componentes eletrônicos do objeto inteligente.
4. Unidade de sensores e atuadores: Eles realizam o monitoramento de grandezas físicas do mundo real como temperatura, pressão, presença, entre outros e os convertem em um sinal analógico que então é recebido pelo microcontrolador e então enviado através do canal de comunicação para o lugar requerido.

 A partir dessas definições é possível entender a arquitetura básica para a construção de um objeto inteligente que faz uso da internet das coisas e o quão amplo são as aplicações possíveis com a IOT, desde simplesmente ler a temperatura de uma sala a partir de um sensor até mesmo desenvolver uma tranca que utiliza a tecnologia de RFID para garantir a segurança de uma organização ou empresa (SANTOS;SILVA;CELES, Não Sei).

# 3.2 Identificação por radio frequencia (RFID)

# 3.2 Protocolo de comunicação MQTT

# Referências

ASSAD, R. E. **Gerenciamento de políticas de segurança para redes de computadores, baseado em ferramentas de auditoria de sistemas**. 2005. 119 f. Dissertação (Mestrado em Ciência da Computação) – Centro de informática da Universidade Federal do Pernambuco, Universidade Federal do Pernambuco, Recife, 2002.

FERNANDES, D. W. **Segurança na internet*?*** 2000. 203 f. Dissertação (Mestrado em Engenharia de produção) – Colegiado do Curso de Mestrado em Engenharia de Produção, Universidade Federal de Santa Catarina, Florianópolis, 2000.

SILVA-NETTO, A.; SILVEIRA, M. A. P. Gestão da segurança da informação: Fatores que influenciam sua adoção em pequenas e médias empresas. **Revista de Gestão da Tecnologia e Sistemas de Informação**, São Paulo, v. 4, n. 3, p. 375-397, 2007.

DIAS, J. M. F.; RODRIGUES, R. C. M. C.; PIRES, D. F. A segurança de dados na computação em nuvens nas pequenas e médias empresas. **Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica**, São Paulo, v. 2, n. 1, 2012.

ABNT - Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 17799:2005**: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005. 116 p.

CAMPOS-FILHO, M. P. Os sistemas de informação e as modernas tendências da tecnologia e dos negócios. **Revista de administração de empresas**, São Paulo, v. 34, n. 6, p. 33-45, 1994.

LYRA, M. R. (org.). **Governança da segurança da informação**. 1. ed. Brasília: 2015, 145 p.

DANTAS, M. L. **Segurança da informação: Uma abordagem focada em gestão de riscos**. 1. ed. Olinda: 2011, 152 p.

SCHNEIER, B. **Segurança.com – segredos e mentiras sobre a proteção na vida digital**. 1. ed. Rio de Janeiro: Editora Campus, 2001.

ADACHI, T. **Gestão de Segurança em Internet Banking**. 121 p. Dissertação (Mestrado em administração de empresas) - Fundação Getúlio Vargas, São Paulo, 2004.

MCROBERTS, M. **Arduino Básico**. 1. ed. São Paulo: Novatec Editora, 2011. 443 p.

FILIPEFLOP. Controle de acesso usando leitor RFID com Arduino. 2014. Disponível em: https://www.filipeflop.com/blog/controle-acesso-leitor-rfid-arduino/. Acesso em: 23 out. 2019.

PFSENSE. pfSense. Disponível em: https://www.pfsense.org/. Acesso em: 17 out. 2019

NEVES F. C.; MACHADO L. A.; CENTENARO R. F. **Implantação de firewall pfSense**. 2014. 66 f. Trabalho de Conclusão de Curso (Graduação em Tecnologia em Sistemas de Telecomunicações) - Universidade Tecnológica Federal do Paraná, Paraná.

WITTS, J. The top 5 Biggest Cyber Security Threats That Small Businesses Face And How To Stop Them. 2021. Disponível em: https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/. Acesso em: 1 nov. 2021.

file:///C:/Users/igor\_/OneDrive/Área%20de%20Trabalho/Faculdade/Projeto%20integrador%202/Artigos%20Mapeados/Engenharia%20social%20nas%20redes%20sociais%20online.pdf

<https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>

file:///C:/Users/igor\_/OneDrive/Área%20de%20Trabalho/Faculdade/Redes%201/Redes%20De%20Computadores%20E%20A%20Internet%20-%20Kurose%20-%206ª%20Ed%20-%20Pdf-1.pdf

Os dois livros do stallings.

file:///C:/Users/igor\_/OneDrive/Área%20de%20Trabalho/Faculdade/Projeto%20integrador%202/Artigos%20Mapeados/Segurança%20da%20informação/Gestão%20da%20Segurança%20da%20Informação%20Uma%20Visão%20Executiva.pdf

file:///C:/Users/igor\_/OneDrive/Área%20de%20Trabalho/Faculdade/Projeto%20integrador%202/Artigos%20Mapeados/Segurança%20da%20informação/2966-14475-1-PB.pdf

file:///C:/Users/igor\_/OneDrive/Área%20de%20Trabalho/Faculdade/Projeto%20integrador%202/Artigos%20Mapeados/Segurança%20da%20informação/ADI-B3180.pdf

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. Segurança em Informática e de Informações – São Paulo: Editora SENAC São Paulo, 1999.

<http://35.238.111.86:8080/jspui/bitstream/123456789/329/1/Santos_Bruno_Internet%20das%20coisas.pdf>

<https://www.researchgate.net/profile/Marcelo-Alves-9/publication/334443396_Plataformas_para_a_Internet_das_Coisas/links/5d29c3a6a6fdcc2462daef7f/Plataformas-para-a-Internet-das-Coisas.pdf>

file:///C:/Users/igor\_/OneDrive/Área%20de%20Trabalho/Faculdade/Projeto%20integrador%202/Artigos%20Mapeados/Hardware/41-Texto%20do%20artigo-215-1-10-20160513.pdf

<https://patricia-gomes-germano.webnode.com/_files/200000030-0936e0a304/Internet%20das%20Coisas%20-%20IOT%20Talyta%20Singer.pdf>

<https://www.researchgate.net/profile/Mauro-Fazion-Filho/publication/319881659_Internet_das_Coisas_Internet_of_Things/links/59c038d5458515e9cfd54ff9/Internet-das-Coisas-Internet-of-Things.pdf>

<https://www.scielo.br/j/cebape/a/mBqjGxPSbRKPsXcS99z8LrD/?lang=pt&format=pdf>