Relatório de Estágio

Ana Cristina Teixeira Antunes

Curso Técnico Superior Profissional em Cibersegurança

set | 2023

GUARDA
POLI
TÉCNICO

Escola Superior de Tecnologia e Gestão

SEGURANÇA DOS EQUIPAMENTOS IOT EM AMBIENTE HOSPITALAR

RELATÓRIO DE ESTÁGIO
PARA OBTENÇÃO DO DIPLOMA DE TÉCNICO(A) SUPERIOR PROFISSIONAL EM CIBERSEGURANÇA

Ana Cristina Teixeira Antunes

Setembro 2023

Escola Superior de Tecnologia e Gestão

SEGURANÇA DOS EQUIPAMENTOS IOT EM AMBIENTE HOSPITALAR

RELATÓRIO DE ESTÁGIO
PARA OBTENÇÃO DO DIPLOMA DE TÉCNICO(A) SUPERIOR PROFISSIONAL EM CIBERSEGURANÇA

Professor(a) Orientador(a): Paulo Nunes

Ana Cristina Teixeira Antunes

Setembro 2023

Agradecimentos

É com enorme orgulho, dedicação e desempenho que termino esta etapa da minha vida académica. Nada seria possível sem a ajuda e incentivo de todos os que percorreram este caminho comigo, a quem gostaria de agradecer por me ajudarem direta ou indiretamente nesta fase da minha vida e por me incentivarem a fazer melhor.

Em primeiro lugar, quero agradecer ao meu marido e aos meus filhos, que sempre me motivaram, apoiaram e me transmitiram forças para me focar no trabalho e no meu futuro, e nunca me deixaram desistir quando aparecia um obstáculo no caminho.

Agradeço ao Instituto Politécnico da Guarda e aos seus professores pelo que me transmitiram durante todo o curso, em especial, ao meu orientador de estágio, professor Paulo Nunes, por ter aceitado este cargo, e claro por todo o apoio e disponibilidade prestado ao longo deste curso, e a todos os outros docentes pela aprendizagem.

Por último quero agradecer à equipa do serviço de informática da ULSG, por terem sido tão prestáveis comigo durante estes meses, por me ajudarem nos momentos em que eu mais precisei e por me ensinarem sempre mais, aumentando assim as minhas capacidades e habilidades na área da informática. Ao Engenheiro Ricardo Santos, gostaria de fazer um especial agradecimento pela sua disponibilidade e compreensão ao longo desta etapa. Agradeço ao Miguel Aguiar pela aprendizagem e conhecimento, pelo companheirismo e amizade e por todas as experiências partilhadas ao longo deste percurso. Ao Engenheiro Luís Domingos, agradeço a partilha de sabedoria e competências na área de segurança e redes.

Agradeço ao António Xavier pela aprendizagem e apoio demonstrado nas áreas de redes e comunicações. Agradeço ainda ao Joel, pois foi com ele que aprendi todas as bases de hardware tão essenciais para esta jornada. Por último, agradeço à Andreia pelos ensinamentos em software e hardware de Impressoras.

Ficha de Identificação

Nome: Ana Cristina Teixeira Antunes

Número: 1008882

Curso: TeSP de Cibersegurança

Contacto: ana.c.t.antunes@gmail.com

Estabelecimento de ensino:

Instituição: Instituto Politécnico da Guarda

Escola de Ensino: Escola Superior de Tecnologia e Gestão

Localidade: Guarda

Morada: Avenida Dr. Francisco Sá Carneiro, nº50, 6300-559

Contacto: 271 220 120; E-mail: estg-geral@ipg.pt; Website: www.estg.ipg.pt

Empresa Acolhedora:

Empresa: ULS-Guarda

Localidade: Guarda

Morada: Av. Rainha Dona Amélia 19, 6300-035 Guarda

Contacto: 271 200 200; E-mail: secretariado.ca@ulsguarda.min-saude.pt

Orientador:

Dr. Paulo Nunes

Supervisor

Ricardo Santos - Diretor do Serviço de Sistemas e Tecnologias da Informação e Comunicações ULS

Duração do Estágio Curricular:

750 Horas

Período de Estágio Curricular:

13 de fevereiro 17 de julho

Resumo

No âmbito de finalizar o Curso de Técnico Superior Profissional em Cibersegurança no Instituto Politécnico da Guarda (IPG), foi desenvolvido o presente relatório de estágio curricular do ano letivo 2022/2023. O período de estágio decorreu no departamento de informática da ULS da Guarda, teve início no dia 13/02/2023 e terminou a 17/07/2023.

A instituição acolhedora deu as condições necessárias para o desenvolvimento e prática das aptidões adquiridas ao longo do plano curricular e novos fundamentos.

Realizadas as apresentações, definimos o plano de estágio e o local de trabalho.

O plano elaborado teve em consideração as necessidades da instituição. O presente relatório irá abordar de forma intensiva um estudo sobre a segurança dos equipamentos IOT em ambiente hospitalar. Este tema foi abordado pelo responsável da Cibersegurança, que referiu ser uma mais-valia a adoção de regras de implementação dos equipamentos IOT.

À parte deste projeto, foi elaborado um manual de boas práticas de Cibersegurança e criada uma página web no Intranet da ULS de informação ao utilizador.

Ao longo do estágio foram realizadas, também, várias tarefas de reparação, configuração e instalação de diversos equipamentos informáticos, tais como impressoras e computadores, bem como a resolução de problemas informáticos (Software e Hardware) comunicados pelos colaboradores.

Plano de estágio

Tendo em conta as necessidades da ULS foi elaborado o seguinte plano:

- Elaboração de manual de boas práticas ao utilizador;
- Criação de página intranet, ULSG Segura;
- Apoio técnico aos utilizadores da instituição da ULS Guarda em caso de alguma avaria;
- Manutenção de Hardware.

A pedido do engenheiro Luís Domingos, responsável pelo departamento de cibersegurança, foi efetuado um estudo relacionado com a segurança dos equipamentos IOT em ambiente hospitalar.

Entidade de acolhimento - Unidade local de Saúde da Guarda

Associada à vida do Sanatório e da própria cidade foi criado o Hospital Sousa Martins, primeiro como sanatório para a cura da tuberculose pulmonar da Europa, inaugurado em 18 de maio de 1907. Mais recentemente, foi integre como Unidade Local de Saúde na Guarda.

A ULS Guarda, EPE tem como missão proporcionar serviços públicos de saúde que permitam a maior abrangência de cuidados à população da sua área de influência e a todos os cidadãos em geral, num projeto partilhado e global que vise a obtenção de Qualidade, Acessibilidade, Eficácia e Eficiência, contribuindo também para o futuro sustentável do SNS. Desenvolve ensino e investigação de alta responsabilidade, por integrar a Faculdade de Ciências da Saúde da Universidade da Beira Interior e colaborar com as Escolas Superiores de Enfermagem e Escolas Superiores de Tecnologias da Saúde e diferentes estabelecimentos de ensino secundário, superior e universitário.

No desenvolvimento da sua atividade, a ULS Guarda, e os seus colaboradores regem-se pelos seguintes princípios:

• Legalidade, Igualdade, Proporcionalidade, Colaboração e boa-fé;

• Humanismo no relacionamento com os utentes e colegas de trabalho;
• Respeito pela dignidade humana;
• Qualidade nas prestações, com níveis de serviço e de resultados elevados;

• Competência e da responsabilidade.

Os Valores que orientam o comportamento e a atuação a ULS Guarda, são:

• Atitude centrada no doente e na promoção da saúde pública e da comunidade, respeitando os valores do cidadão e da família;
• Cultura de excelência técnica, científica e do conhecimento, como um valor a prosseguir continuamente;
• Cultura interna de multidisciplinaridade e de bom relacionamento no trabalho;
• Responsabilidade Social, contribuindo para a otimização na utilização dos recursos e da capacidade instalada.

O serviço de sistemas de informação e comunicação da ULS mais conhecido por informática, situa-se no andar abaixo da maternidade perto do antigo sanatório.
O centro de informática tem um papel fundamental no Hospital e nos restantes centros de saúde do distrito, pois é lá que tudo é gerido, monitorizado e efetuadas as manutenções e reparações.

Índice

Lista de Figuras

Lista de tabelas

Lista de siglas e acrónimos

2FA	Two Factor Authetication / Dois fatores de autenticação
API	Application Programming Interface
CoAP	Constrained Application Protocol
CNC	Centro Nacional de Cibersegurança
CSRF	Cross-site request forgery
CVE	Common Vulnerabilities and Exposures
DICOM	Digital Imaging and Communications in Medicine
DoS	Denial Of Service
ECG	Eletrocardiograma
ESTG	Escola Superior de Tecnologia e Gestão
HL7	Health Level Seven
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IDS	Intrusion detection system
IoT	Internet of things
IP	Internet Protocol.
IPS	Intrusion prevention system
IPv6	Internet Protocol v6
LAN	Local Area Network
MAN	Metropolitan Area Network
MQTT	Message Queue Telemetry Transport
NFC	Near Field Communication
PACS	Picture Archiving and Communication System
PAN	Personal Area Network
QGBT	Quadro geral de baixa tensão
RFID	Radio Frequency Identification
RGPD	Regime Geral de Proteção de Dados
SD	Secure Digital Card
SIEM	Security Information and Event Management
SMS	Short Message Service

1.Introdução

Nos últimos anos, o setor de saúde demonstrou grande entusiasmo em adotar a Internet das Coisas (IoT). Esses dispositivos inteligentes têm um potencial significativo para melhorar diagnósticos, tratamentos e salvar vidas ao recolher e analisar dados médicos anteriormente inacessíveis. Eles permitem que os profissionais de saúde ofereçam tratamentos personalizados e essenciais de maneira mais eficiente, com monitoramento ativo e contínuo.

No entanto, essa crescente adoção da tecnologia IoT na área de saúde também apresenta preocupações significativas relacionadas à integridade de dados sensíveis dos pacientes e à operação contínua e confiável dos sistemas. É necessário que os dispositivos de IoT protejam os dados que recolhem, transmitem e armazenam, garantindo que permaneçam seguros contra possíveis interceções. Isto significa que se não forem desenhados e construídos tendo como principal premissa a sua segurança, é muito provável que em breve venham a tornar-se vulneráveis e a comprometer a saúde e segurança do doente.

Num mundo cada vez mais digital, as equipas de tecnologia da informação de várias instituições e organizações precisam estar atentas às mudanças tecnológicas que podem afetar os seus negócios. Conforme a IoT se prolifera pela sociedade recolhendo cada vez mais dados a partir de objetos, máquinas e pessoas, as organizações enfrentam novas oportunidades, riscos e desafios de segurança que precisam ser tratados adequadamente.

Na área da saúde, a adoção dessas tecnologias tem acompanhado essa tendência global, com a proliferação de equipamentos médicos conectados. No entanto, essa proliferação também traz diversos riscos e vulnerabilidades. A IoT pode revolucionar a assistência médica, mas também pode abrir portas para cibercriminosos e indivíduos mal-intencionados que visam o lucro financeiro, mesmo que isso coloque em risco a disponibilidade e a segurança dos pacientes.

Em ambientes hospitalares e unidades de saúde, é essencial monitorizar constantemente os ativos conectados à rede, uma vez que pequenos erros ou problemas podem ter consequências graves. A IoT pode ser uma ferramenta valiosa para equipas multidisciplinares, fornecendo informações em tempo real e alertas em caso de eventos críticos.

Embora muitas unidades de saúde ainda dependam de processos manuais e registos em papel, a IoT está a alterar esse paradigma, permitindo a recolha de dados com maior precisão e eficácia por meio de sensores e dispositivos automatizados.

À medida que a IoT se expande, os benefícios para as instituições de saúde são evidentes, mas também surgem novos riscos de segurança e privacidade. Os dispositivos IoT enfrentam vulnerabilidades na comunicação devido à sua infraestrutura variável e recursos limitados. Este trabalho aborda a falta de segurança em dispositivos IoT, destacando os riscos e vulnerabilidades específicos que esses dispositivos em unidades de saúde podem enfrentar, juntamente com boas práticas para sua implementação em ambientes sensíveis como hospitais, clínicas e laboratórios.

1.1. Objetivos e contribuições

Este estudo tem como foco principal a segurança e os frequentes ataques que têm afetado os dispositivos conectados às redes das unidades de saúde. Os objetivos principais incluem a identificação e a definição de procedimentos de boas práticas e mecanismos de segurança para os equipamentos de saúde.

Após uma análise abrangente do estado da arte e uma compreensão das várias formas de comunicação dos dispositivos IoT, foram identificados os tipos de ameaças e os ataques mais comuns que estes dispositivos enfrentam. Além disso, foram detalhados os principais métodos de comunicação, protocolos amplamente utilizados e as normas associadas a estes equipamentos.

A primeira contribuição deste trabalho envolve a caracterização dos principais equipamentos utilizados em unidades de saúde, com ênfase nos dispositivos IoT que estão conectados à rede e geram informações, incluindo informações sensíveis ou confidenciais.

A segunda contribuição concentra-se na identificação dos principais riscos que os dispositivos IoT enfrentam em ambientes de saúde, destacando os riscos mais conhecidos associados ao uso desses equipamentos.

A terceira contribuição destaca as vulnerabilidades mais comuns que podem ser encontradas nos dispositivos IoT em instituições de saúde, com ênfase na segurança do paciente e na proteção dos dados gerados diariamente.

Com base nessas contribuições, foram definidos procedimentos e diretrizes de boas práticas para a implementação segura desses dispositivos em unidades de saúde.

No último capítulo, são apresentadas as conclusões deste estudo e discutidas medidas preventivas, bem como possíveis direções para trabalhos futuros.

1.2. Estrutura

Neste trabalho, que visa alcançar os objetivos e contribuições previamente definidos, a estrutura é organizada da seguinte forma:
No Capítulo 2, é apresentado o estado da arte da cibersegurança, fornecendo uma visão geral das tendências e desafios neste campo.

O Capítulo 3 aborda especificamente a cibersegurança no contexto da Internet das Coisas (IoT), incluindo os tipos de comunicação usados por estes dispositivos. São discutidas as motivações por trás dos ataques à segurança de equipamentos em unidades de saúde, bem como os diversos tipos de ataques de segurança conhecidos e as principais ameaças associadas a estes dispositivos.

No Capítulo 4, é realizada uma caracterização detalhada dos principais equipamentos utilizados em unidades de saúde que representam potenciais riscos para a segurança e integridade das informações neste ambiente. Este capítulo também analisa os principais riscos dos equipamentos IoT, incluindo preocupações relacionadas à recolha em massa de dados, confidencialidade, fiabilidade, controlo de acessos, middleware inseguros, redes programáveis, ataques baseados em botnets, falhas de energia, big data, malware, interoperabilidade, falsificação e pontos de acesso. Além disso, são destacadas as principais vulnerabilidades destes dispositivos, abordando questões como acesso remoto, testes de penetração, ataques de força bruta, passwords fracas, backdoors, firmware inseguro e ausência de adoção de padrões.

No Capítulo 5, são apresentadas regras e boas práticas para a implementação segura de equipamentos IoT em unidades de saúde. Isso inclui orientações para fortalecer a segurança da rede e capacitar os profissionais que interagem com estes dispositivos no seu quotidiano, garantindo um ambiente livre de problemas que possam comprometer a continuidade das operações.

O Capítulo 6 consiste na conclusão do trabalho, onde são resumidas as principais conclusões e são fornecidas indicações para futuras investigações e desenvolvimentos.
Finalmente, no capítulo 7, como anexo, apresento o manual de boas práticas ao utilizador na cibersegurança, bem como página intranet para alojar num servidor local da ULS.

2.Estado da arte da Cibersegurança

O estado da arte da cibersegurança é uma área em constante evolução devido à crescente complexidade das ameaças digitais e ao avanço tecnológico. Neste contexto, é fundamental manter-se atualizado sobre as tendências e os desafios em constante mudança para proteger sistemas, dados e informações contra ameaças cibernéticas. Aqui estão alguns tópicos relevantes no estado da arte da cibersegurança:

Aumento das Ameaças Cibernéticas: As ameaças cibernéticas estão cada vez mais sofisticadas e diversificadas, incluindo ataques de ransomware, phishing, malware avançado e ataques direcionados. Os cibercriminosos exploram novos vetores de ataque, como dispositivos IoT e sistemas em nuvem.

Inteligência Artificial e Machine Learning: A inteligência artificial (IA) e a aprendizagem de máquina estão a ser usadas tanto por cibercriminosos quanto por defensores da cibersegurança. Isso inclui a deteção de ameaças em tempo real, análise comportamental e automação de tarefas de segurança.

Internet das Coisas (IoT): A proliferação de dispositivos IoT aumentou a superfície de ataque. A segurança dos dispositivos IoT é uma preocupação, uma vez que muitos deles têm vulnerabilidades de segurança significativas.

Nuvem e Virtualização: A migração para ambientes em nuvem e a virtualização de recursos de TI introduzem novos desafios de segurança, incluindo a gestão de identidade e acesso, a proteção de dados e a segurança da infraestrutura em nuvem.

Privacidade dos Dados: As regulamentações de privacidade de dados, como o RGPD na União Europeia e a Lei de Privacidade do Consumidor da Califórnia (CCPA), estão a aumentar a importância da proteção de dados pessoais. As empresas precisam adotar medidas de segurança mais rigorosas para cumprir essas regulamentações.

Zero Trust Security: O modelo de segurança Zero Trust, que assume que não se pode confiar automaticamente em utilizadores ou dispositivos dentro ou fora da rede, está a ganhar destaque. A autenticação multifatorial e a segmentação de rede são componentes-chave desse modelo.

Hacking Ético e Testes de Penetração: A demanda por profissionais de segurança cibernética, incluindo hackers éticos e especialistas em testes de penetração, está em alta. As organizações procuram identificar vulnerabilidades nos seus sistemas antes que os cibercriminosos o façam.

Cibersegurança Industrial (ICS/SCADA): A proteção de sistemas de controlo industrial e sistemas de aquisição de dados (ICS/SCADA), como energia, água e transporte é crítica. Ataques direcionados a estes sistemas podem ter consequências devastadoras.

Consciencialização do Utilizador: A educação e a consciencialização do utilizador são componentes essenciais da cibersegurança. As empresas investem em formação aos funcionários, para que possam identificar ameaças e praticar comportamentos seguros online.

Resposta a Incidentes e Recuperação: É crucial ter planos de resposta a incidentes sólidos para mitigar os danos causados por ataques cibernéticos. A capacidade de recuperação de dados e sistemas após um incidente também é fundamental.

Blockchain e Criptomoedas: A tecnologia blockchain tem o potencial de melhorar a segurança de transações e sistemas. No entanto, também é utilizada em esquemas de criptomoedas e contratos inteligentes, que podem ser alvo de ataques.

Regulamentações e Conformidade: As regulamentações de cibersegurança continuam a evoluir, e as empresas precisam estar em conformidade com as leis e regulamentações específicas da sua indústria e localização geográfica.

O estado da arte da cibersegurança está intrinsecamente ligado ao panorama tecnológico em constante evolução e às ameaças em constante mudança. A cibersegurança é uma prioridade crescente para empresas e governos, à medida que todos dependemos cada vez mais da tecnologia digital nas nossas vidas cotidianas. Portanto, a pesquisa e o desenvolvimento contínuos são essenciais para acompanhar as ameaças e proteger ativos digitais críticos.

2.1. Definição de cibersegurança

A transformação digital tem levado indivíduos e organizações a uma crescente dependência das Tecnologias de Informação. Como resultado dessa transformação, a Internet tornou-se essencial, dando origem ao conceito de Ciberespaço. A vantagem do uso do Ciberespaço é a sua natureza livre e aberta, tornando-o acessível a qualquer pessoa ou organização que deseje aproveitar os seus benefícios.

De acordo com o CNCS, a cibersegurança é definida como um conjunto de medidas e ações essenciais para prevenir, detetar e analisar sistemas de informação. Essas medidas visam garantir a integridade, disponibilidade e confidencialidade dos dados.

A Microsoft, por sua vez, conceitua cibersegurança como a proteção de informações digitais, dispositivos e recursos.

Conforme a APDSI, a cibersegurança envolve um conjunto de meios voltados para a segurança de programas, computadores, redes e dados, prevenindo qualquer intrusão não autorizada. A base dessa segurança está na integridade, confidencialidade e disponibilidade da informação.

De acordo com a IBM, a cibersegurança concentra-se na proteção de sistemas críticos e informações sensíveis contra incidentes de segurança, com medidas projetadas para conter ameaças a esses sistemas e dados críticos.

Existem várias propostas para definir o conceito de cibersegurança, mas talvez a abordagem mais eficaz seja combinar duas ou mais dessas definições. necessário estabelecer normas que garantam a segurança daqueles que utilizam o ciberespaço. Essas normas e boas práticas visam impedir o uso não autorizado do ciberespaço e auxiliar as organizações na implementação das medidas necessárias para cumprir as melhores práticas de cibersegurança.

Essas normas representam instrumentos à disposição de todas as organizações para lidar com diversos riscos de segurança e descrevem as melhores práticas para torná-las mais resilientes. Cada organização deve avaliar e selecionar as normas que melhor se adequam ao seu negócio, dependendo dos processos que ela segue.

Dado que a cibersegurança é uma área de crescente preocupação para os responsáveis nas organizações, é crucial avaliar o nível de maturidade em cibersegurança em que se encontram.

A identificação precoce de possíveis lacunas e vulnerabilidades por meio de diversos tipos de testes é fundamental para prevenir incidentes de segurança.

2.2. Normas, leis e boas práticas da cibersegurança

Diante dos desafios e ameaças apresentados, surgiu a necessidade de criar um documento ou guia que capacitasse e apoiasse organizações e cidadãos na adoção de boas práticas relacionadas a essa questão.

Em 2016, o National Institute of Standards Technology (NIST) [1] publicou a primeira versão da NISTIR 7621, intitulada "Small Business Information Security: The Fundamentals". Este guia foi especialmente desenvolvido para pequenas e médias empresas (PMEs), que muitas vezes acreditam que, devido ao seu tamanho reduzido, não estão suscetíveis a incidentes de cibersegurança. O foco deste guia é explicar os princípios básicos de cibersegurança que as organizações devem adotar para proteger as suas informações e ativos.

Essa estrutura oferece uma solidez com base nos padrões, diretrizes e práticas do setor privado dos Estados Unidos. Ela auxilia as organizações na implementação de mecanismos de prevenção e deteção, além de fornecer orientações sobre como agir em caso de incidentes de cibersegurança. Como resultado, observou-se uma melhoria na comunicação entre as organizações e as entidades às quais os incidentes devem ser relatados.

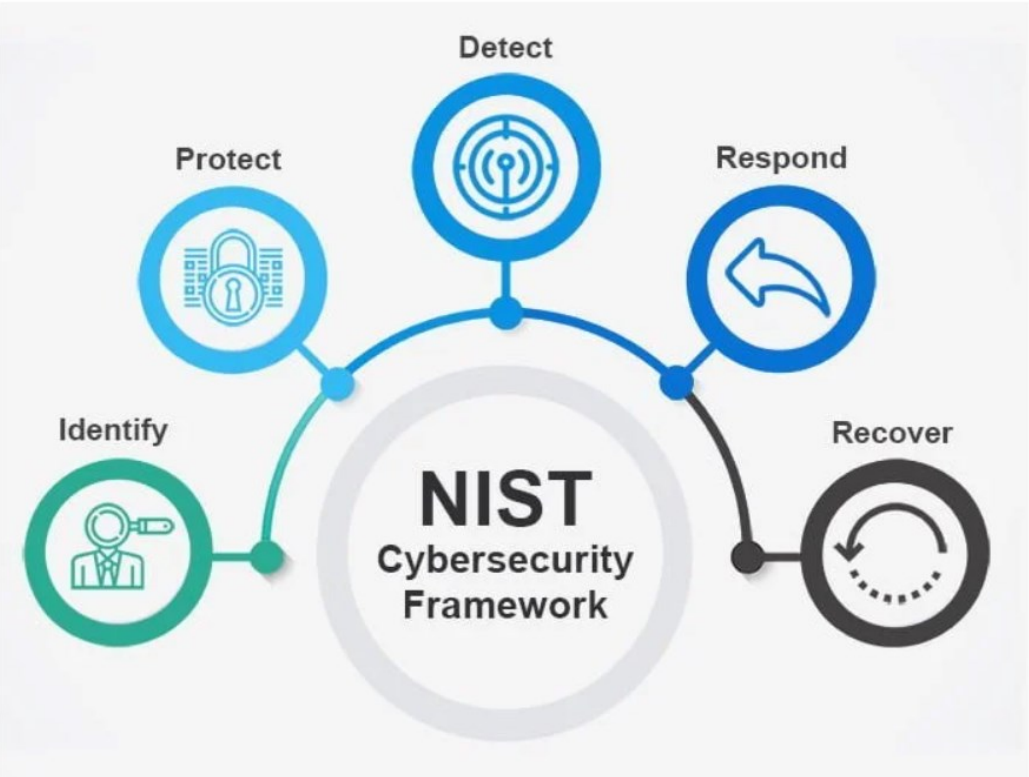

Figura 1 - As cinco funções da framework NIST

Na Figura 1, encontram-se representadas as cinco funções-chaves de segurança destinadas a organizar os controlos de segurança.

A estrutura proposta no documento [2] consiste em três elementos centrais, a saber: o núcleo, o perfil e os níveis de implementação da estrutura.

O núcleo é composto por um conjunto de atividades e resultados desejados em cibersegurança, destinados a manter uma conexão com a gestão de riscos, utilizando uma linguagem de fácil compreensão.

Na parte do perfil, são selecionadas várias funções, categorias e subcategorias específicas do núcleo, escolhidas para apoiar a organização na gestão de risco de privacidade. O perfil tem como objetivo melhorar os padrões de segurança e mitigar os riscos na organização.

Quanto à última componente, os níveis de implementação auxiliam na tomada de decisões organizacionais sobre como gerir o risco da privacidade. Eles determinam o nível de rigor apropriado para a organização e fornecem um contexto sobre a robustez da estratégia de cibersegurança da organização.

O propósito desta norma é estabelecer um conjunto de controlos de segurança básicos voltados para informações, sistemas e redes. A estrutura serve como ponto de referência e apoio para as organizações, usando um vocabulário de fácil leitura e compreensão.

2.3. Diretiva NIS2

A Diretiva de Segurança de Redes e Informação (NIS) [3] representou a primeira legislação da União Europeia relacionada com cibersegurança. O principal objetivo desta legislação é estabelecer um nível consistente de segurança cibernética em todos os países da Europa e fortalecer a cibersegurança em toda a União Europeia. Devido à sua natureza como legislação europeia, cada país da UE desenvolveu as suas próprias regulamentações com base nessa diretriz.

Em Portugal, a Lei nº 46/2018 foi promulgada para estabelecer o quadro jurídico da segurança cibernética, incorporando as disposições da mencionada Diretiva (UE) 2016/1148. Essa lei nacional visa a transposição da diretiva europeia para o contexto nacional.

Figura 2- Áreas de atuação da Diretiva NIS [4]

Na Figura 2 pode-se observar uma síntese da diretiva, composta por três partes distintas que são representadas.

Nas capacidades nacionais está mencionado que cada país deve dispor de determinadas capacidades nacionais, como um CSIRT nacional [5] , executar simulacros e exercícios de treino para a preparação nesta matéria, entre outros.
Na segunda área é definido que deve existir colaboração entre os países da UE.
É recomendado que seja estabelecida uma comunicação com a rede operacional CSIRT da União Europeia ou com o grupo estratégico de cooperação NIS.

A última área refere que a cibersegurança dos mercados críticos de cada país deve ser supervisionada, por exemplo, o setor da energia, transportes, água, saúde, infraestruturas digitais e setor financeiro. O grupo de orientação desta diretiva, fornece orientação estratégica à rede CSIRT da EU

2.4. Controls (Center for Internet Security)

O Center for Internet Security (CIS) [6] é um conjunto de diretrizes de boas práticas para a segurança da informação, lançado em 2008 em resposta aos desafios crescentes de cibersegurança. O CIS é uma organização sem fins lucrativos com renome internacional na área da cibersegurança, conhecida por ajudar a encontrar as melhores defesas contra-ataques cibernéticos.

O conjunto de diretrizes consiste em 171 controlo que podem ser aplicados em 20 áreas distintas. Esses controlos são divididos em três grupos distintos:

- **Controlos Básicos;**
- **Controlos Essenciais;**
- **Controlos Organizacionais.**

Inicialmente, o objetivo era modesto, ou seja, auxiliar pessoas e organizações a dar os primeiros passos em segurança. No entanto, os CIS Controls evoluíram significativamente ao longo do tempo e tornaram-se numa comunidade de voluntários, tanto indivíduos quanto instituições, que:

- Partilham conhecimentos e experiências sobre ataques e atacantes, identificando causas raiz e traduzindo-as em ações defensivas;
- Desenvolvem e partilham ferramentas e soluções para problemas existentes;
- Mapeiam os controlos CIS com estruturas regulatórias para alinhá-los com prioridades e foco;
- Identificam problemas e barreiras comuns, como avaliação inicial e planos de implementação.

Os CIS Controls são utilizados em diversas indústrias, incluindo saúde, educação, governo, entre outras, devido à sua capacidade de se adaptar a organizações de todos os tamanhos e setores. Uma característica distintiva é a capacidade de não apenas bloquear sistemas

comprometidos, mas também detetar dispositivos já comprometidos e prevenir ameaças futuras. Implementar esses controlos é uma vantagem para avaliar e melhorar o nível de segurança de uma organização e identificar áreas de melhoria.

Os controlos estão divididos em três grupos de implementação adequados para diferentes tipos de organizações e níveis atuais de segurança. Por exemplo, uma organização que não possui controlos de segurança deve começar pela implementação do IG1 e progredir gradualmente.

A Figura 3 [7] mostra que os IGs (Grupos de Implementação) dos controlos CIS são categorias autoavaliadas para organizações. Cada IG identifica um subconjunto dos controlos CIS escolhidos e avaliados como aplicáveis a uma organização com perfil de risco e recursos semelhantes. Esses IGs representam uma visão horizontal dos controlos CIS e são adaptados a diferentes tipos de empresas.

O Grupo de Implementação IG1 é conhecido como "Higiene Cibernética Básica" e consiste num conjunto de medidas fundamentais de segurança e proteção que todas as empresas devem adotar para se resguardarem contra os ataques mais comuns. Cada subgrupo de IGs subsequente baseia-se no anterior, o que significa que o IG2 engloba todas as medidas do IG1, e o IG3 engloba todas as medidas do IG1 e IG2. Para determinar em qual grupo a organização se encontra atualmente, é necessário realizar uma autoavaliação e, com base nos resultados obtidos, alinhar-se com um desses grupos e seguir seus controlos correspondentes.

Figura 3 - Esquema IG's dos controlos CIS

Uma organização de porte pequeno ou médio, com experiência limitada em tecnologia da informação, onde a segurança se concentra principalmente na proteção de ativos e colaboradores da área de TI, enquadra-se no Grupo de Implementação 1 (IG1). O foco principal dessas empresas é manter o negócio operacional, já que não podem suportar longos períodos de inatividade. A quantidade de dados críticos é relativamente baixa e, na sua maioria, consiste em informações financeiras e dados pessoais de funcionários.

Em contraste, uma organização que conta com colaboradores responsáveis pela manutenção da infraestrutura e segurança de TI enquadra-se no Grupo de Implementação 2 (IG2). Estas organizações oferecem suporte a diversos departamentos com diferentes níveis de risco, dependendo de suas respetivas missões. Normalmente, estas organizações armazenam informações confidenciais de clientes ou outras empresas, e têm uma maior tolerância para períodos de inatividade. No entanto, uma das principais preocupações destas organizações é preservar sua reputação em caso de incidentes de cibersegurança.

Por último, uma organização que emprega especialistas em diversas áreas da cibersegurança enquadra-se no Grupo de Implementação 3 (IG3). Os ativos e dados pertencentes a esta categoria estão sujeitos a regulamentações rigorosas de supervisão e conformidade. As organizações deste grupo têm plena consciência de que um ataque bem-sucedido pode causar danos significativos e, portanto, investem consideravelmente em medidas de segurança e conformidade.

2.5. ISO/IEC 27001:2013

A norma ISO 27001:2013 [8] tornou-se uma referência global na gestão da Segurança da Informação, estabelecendo os requisitos de auditoria para um Sistema de Gestão de Segurança da Informação.

Dentro da série ISO27XXX, esta foi a primeira norma publicada pela International Organization for Standardization (ISO) [9] , em outubro de 2005. Suas características permitem que seja adotada por organizações de diversos tipos, independentemente do seu modelo de negócios. A norma é uma evolução direta da norma BS799 do British Standards Institute (BSI) [10] , que foi criada em 1992. Desde então, a ISO 27001 tem passado por várias revisões e beneficia do conhecimento de milhares de profissionais para alcançar um alto nível

de maturidade. A premissa fundamental desta norma é que as organizações devem adotar requisitos, processos e controlos específicos para mitigar e gerir eficazmente os riscos relacionados à segurança da informação.

Muitas organizações procuram a certificação ISO 27001 como um meio de implementar um Sistema de Gestão de Segurança da Informação (SGSI). Ao obter esta certificação, uma organização demonstra conformidade com os requisitos e processos estipulados na norma, aumentando a confiança dos seus clientes em relação à segurança da informação. A obtenção da certificação também reflete o comprometimento e a importância que a organização atribui à segurança da informação.

Para orientar o processo de implementação de um SGSI, a ISO segue o modelo PDCA (Plan, Do, Check, Act). [11]

Figura 4- Modelo PDCA [8]

Na Figura 4, é apresentado o modelo que orienta o funcionamento desta norma:

Plan - Estabelecer o SGSI: Nesta fase, o Sistema de Gestão de Segurança da Informação (SGSI) é criado e planeado. São definidos todos os objetivos e limites do SGSI.

Do - Implementar e Utilizar o SGSI: Durante esta etapa, tudo o que foi definido na fase anterior é colocado em prática. Além disso, a gestão de riscos é realizada, e um plano de tratamento de riscos é desenvolvido. Políticas e procedimentos são estabelecidos para controlar os riscos. É também o momento de iniciar a formação dos colaboradores e implementar as ferramentas necessárias para monitorizar o que está a ser utilizado na organização.

Check - Monitorizar o SGSI: Na terceira fase, ocorre a monitorização e a possibilidade de realizar melhorias na implementação já realizada. Verifica-se se os resultados alcançados estão de acordo com as expectativas.

Act - Manter o SGSI: Por fim, nesta etapa, são aplicadas as medidas necessárias para correção, garantindo que os objetivos iniciais sejam alcançados.

Todos os processos definidos nas quatro fases mencionadas acima devem ser documentados e atualizados regularmente para demonstrar conformidade com os requisitos estabelecidos em cada etapa.

Esta norma é abrangente e adapta-se facilmente a qualquer marca ou fabricante de tecnologia. Além disso, a sua versatilidade torna-a compatível com diversos tópicos, incluindo telecomunicações, segurança de aplicações, proteção de infraestrutura física, gestão de recursos humanos, continuidade de negócios, licenciamento, entre outros.

2.6. Norma ISO/IEC 27701-2019

A norma ISO/IEC 27701 [12] é voltada para a gestão de informações privadas e estabelece requisitos e diretrizes para auxiliar as empresas na gestão de riscos de privacidade relacionados às informações de identificação pessoal. Além disso, fornece orientações específicas sobre como estabelecer, implementar, manter e aprimorar continuamente um Sistema de Gestão de Informações de Privacidade (PIMS). Este PIMS é uma extensão do Sistema de Gestão de Segurança da Informação (ISMS) definido na ISO 27001 e leva em consideração as precauções especiais necessárias para o processamento de dados de Identificação Pessoal (PII) [13] .

Sendo uma norma que estende da ISO 27001 e ISO 27002, no caso de uma organização pretender obter esta certificação um requisito obrigatório é que possua

um sistema de gestão de segurança da informação, implementado segundo a norma ISO 27001.

Uma organização que adere aos requisitos desta norma demonstra como lidar com os dados pessoais, o que pode ser uma vantagem significativa em acordos com parceiros de negócios, especialmente quando a questão da privacidade é de extrema importância.

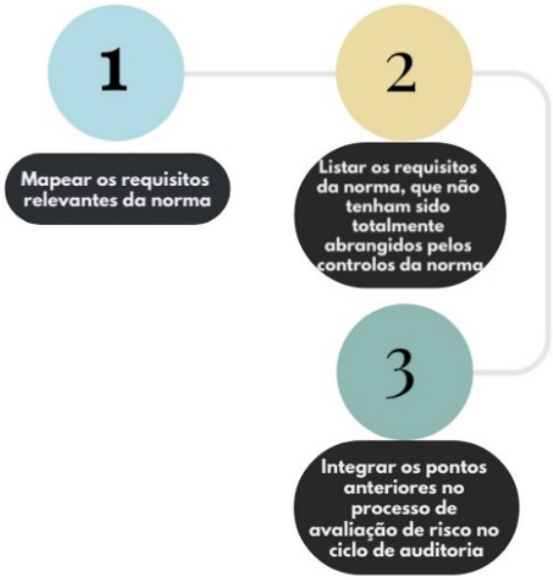

Figura 5- Medidas para avaliar os controlos da norma [12]

A Figura 5 ilustra as medidas essenciais para avaliar os controlos estabelecidos pela norma.

É importante notar que os controlos definidos nesta norma estão alinhados diretamente com os requisitos do Regulamento Geral de Proteção de Dados (RGPD).

Um aspeto distintivo desta norma em relação a todas as outras normas ISO é que ela requer a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) conforme estabelecido pela norma ISO 27001 como um requisito prévio.

Figura 6- Grupos de requisitos da norma ISO 27701 [12]

Na Figura 6 estão representados os grupos de requisitos para que esta norma seja implementada.

2.7. Roteiro para as Capacidades Mínimas de Cibersegurança

O Centro Nacional de Cibersegurança (CNCS) estabeleceu este modelo com o objetivo de capacitar as organizações, especialmente as Pequenas e Médias Empresas (PMEs), visando aprimorar seus processos.

Em resposta ao aumento das atividades de cibercrime, houve a necessidade de criar Centros Nacionais de Cibersegurança e desenvolver estratégias nacionais. Devido à ausência de uma autoridade ou legislação específica em Portugal nesse domínio, o país tomou a decisão de estabelecer uma entidade autoritária dedicada à cibersegurança, dando origem ao Centro Nacional de Cibersegurança (CNCS).

O CNCS atua como a autoridade nacional competente para questões relacionadas à cibersegurança, exercendo autoridade sobre o Estado e infraestruturas críticas. A equipa nacional de resposta a incidentes de cibersegurança, conhecida como CERT.PT, opera sob a supervisão do CNCS e desempenha um papel fundamental na coordenação da resposta a incidentes envolvendo entidades governamentais, prestadores de serviços de telecomunicações, serviços críticos e interesses nacionais em todo o território português.

Este documento [14] , desenvolvido pelo CNCS, fornece um guia de boas práticas que permite que as organizações progridam gradualmente por meio das cinco fases delineadas. Destina-se a ajudar as organizações a cumprir os requisitos mínimos de cibersegurança.

O roteiro está dividido em cinco fases, cada uma delas contendo um conjunto de ações. Essas ações desempenham um papel fundamental no progresso do desenvolvimento. A seguir, serão detalhadas todas as fases e suas respetivas ações.

Fase 1 - Preparação Inicial

A primeira fase visa estabelecer diretrizes para a colaboração entre o Centro Nacional de Cibersegurança (CNCS) e a organização. O principal objetivo nesta etapa é facilitar essa colaboração. As ações definidas nesta fase são as seguintes:

- **Ação 1.1 –** Formalização de Protocolo de Colaboração e Adenda
- **Ação 1.2 –** Identificação do RESPONSÁVEL DE SEGURANÇA
- **Ação 1.3 –** Identificação de funções ou atividades críticas
- **Ação 1.4 –** Estabelecimento de canais de comunicação
- **Ação 1.5 –** Registo de endereços de IP no LIR (Local Internet Registry)
- **Ação 1.6 –** Estabelecimento de metodologia de Análise de Risco
- **Ação 1.7 –** Cadeia de responsabilidade: preparação
- **Ação 1.8 –** Definição de política de segurança de informação
- **Ação 1.9 –** Procedimentos de notificação de incidentes

Estas ações compõem a fase inicial do processo e estabelecem as bases para a colaboração e o desenvolvimento subsequente.

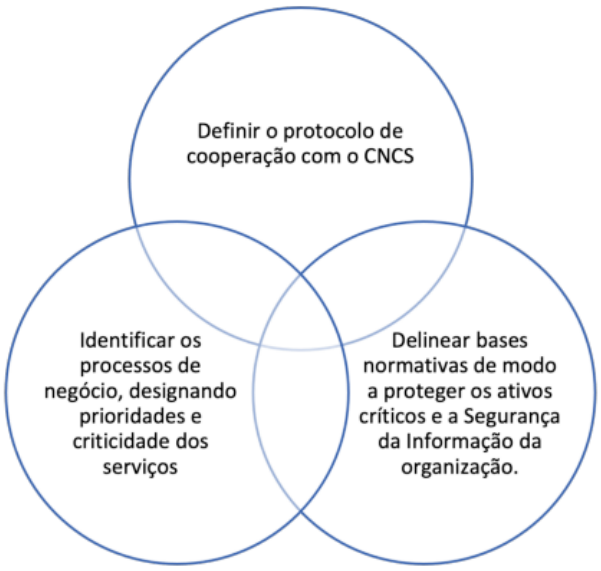

Figura 7- Objetivos para a Fase 1 [14]

Os objetivos desta fase, conforme ilustrado na Figura 8, serão descritos em detalhes a seguir:

- **Definir o protocolo de cooperação com o CNCS:** Nesta etapa, é fundamental formalizar o protocolo de colaboração com o Centro Nacional de Cibersegurança (CNCS). Isso inclui a definição de canais de comunicação a serem utilizados, a elaboração de procedimentos de notificação e a nomeação do responsável pela Segurança.
- **Identificar os processos de negócio, designar prioridades e criticidade dos serviços:** Neste ponto, é necessário identificar todos os processos de negócio da organização. Isto envolve a determinação dos processos prioritários e a atribuição de níveis de criticidade a cada serviço.
- **Estabelecer bases normativas para proteger ativos críticos e a Segurança da Informação da organização:** As bases normativas têm como objetivo principal a proteção dos ativos críticos da organização e da informação interna. Para definir essas bases normativas, é crucial estabelecer uma cadeia de responsabilidade interna para sistemas e ativos, bem como adotar uma metodologia de gestão de risco que aborde a mitigação de ameaças.

Estes objetivos formam a estrutura essencial para a preparação inicial da organização, garantindo que todas as medidas necessárias sejam tomadas para estabelecer uma colaboração eficaz com o CNCS e para proteger os ativos críticos e a segurança da informação da organização.

Fase 2 - Arquitetura

Esta fase consiste num leque de ações recomendadas e baseadas na fase anterior, mas ainda contém ações que permitem dotar a organização das capacidades necessárias para uma defesa eficiente dos seus ativos, em diferentes níveis, nomeadamente, o perímetro da sua rede, servidores, postos de trabalho e outros dispositivos. Ainda nesta etapa é esperado que seja garantida a conformidade essencial da informação com requisitos legais e normativos de acordo com a área de atividade da organização.

Nesta fase estão presentes as seguintes ações:

- **A 2.1 –** Desenho e implementação da arquitetura e segurança perimétrica
- **A 2.2 –** Implementação de sistema de recolha e armazenamento do fluxo de
- tráfego

- **A 2.3 –** Comunicação com o CNCS
- **A 2.4 –** Inventariação de ativos / produção de um mapa de rede
- **A 2.5 –** Recolha centralizada de registos (logs)
- **A 2.6 –** Criação de instrumentos de correção ou mitigação de incidentes
- **A 2.7 –** Estabelecimento de conformidade com a legislação aplicável
- **A 2.8 –** Estabelecimento de conformidade com normas aplicáveis à área de
- atividade
- **A 2.9 –** Criação de política de uso aceitável
- **A 2.10 –** Manutenção de infraestruturas de cópias de segurança e reposição
- (Backup/Restore)
- **A 2.11 –** Mapa de competências e planos de formação
- **A 2.12 –** Treino e sensibilização interna: geral
- **A 2.13 –** Treino e sensibilização interna: gestão

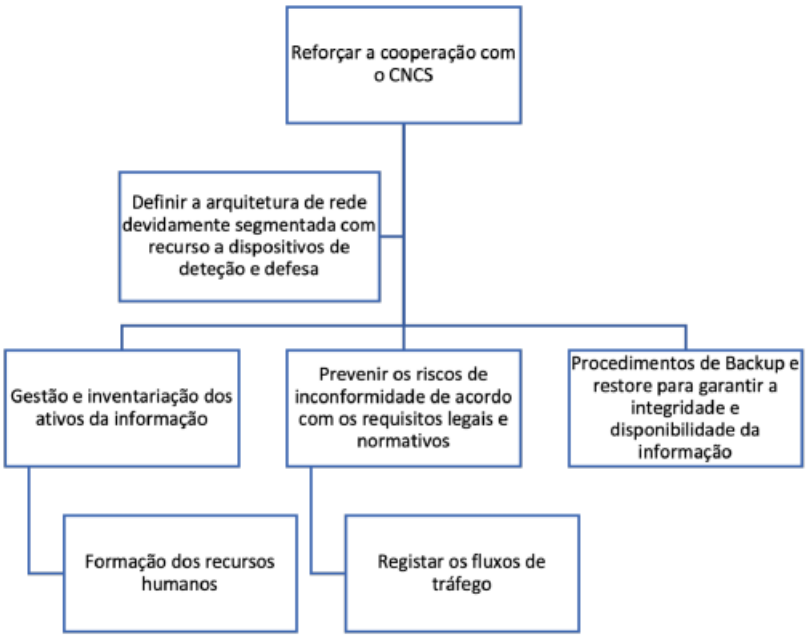

Figura 8- Objetivos para a Fase 2 [14]

Seguidamente serão aprofundados os objetivos desta fase.

- **Reforçar a Cooperação com o CNCS:** Neste ponto, é crucial fortalecer a colaboração com o CNCS, utilizando os canais de comunicação previamente definidos na fase anterior.

- **Definir uma Arquitetura de Rede Adequadamente Segmentada com Dispositivos de Deteção e Defesa:** A arquitetura de rede deve ser devidamente segmentada e equipada com dispositivos de deteção e defesa contra ameaças externas.
- **Registar os Fluxos de Tráfego:** Todos os fluxos de tráfego devem ser registados para permitir uma deteção precoce de eventos de segurança. Além disso, esse registo serve para testar a eficácia dos sistemas internos em resposta a eventos de segurança.
- **Gerir e Inventariar os Ativos de Informação:** Um inventário completo de todos os ativos de informação deve ser elaborado. Isto proporciona à organização uma visão abrangente dos seus recursos internos, permitindo lidar com possíveis ameaças de forma mais eficaz.
- **Estabelecer Procedimentos de Backup e Restauração para Garantir a Integridade e Disponibilidade da Informação:** A organização deve criar procedimentos detalhados de backup e restauração para garantir a resiliência da integridade e disponibilidade das informações críticas.
- **Fornecer Formação aos Recursos Humanos:** A formação e sensibilização devem ser abrangentes e estender-se a todos os colaboradores da organização, de modo que a cibersegurança seja uma responsabilidade partilhada por todos. Isso permitirá que todos os colaboradores estejam cientes e capazes de tomar medidas relacionadas com a segurança cibernética nas suas atividades diárias.

Essa fase tem como objetivo fortalecer ainda mais a postura de segurança da organização, garantindo que a infraestrutura de TI esteja preparada para lidar com ameaças externas e que todos os colaboradores estejam conscientes e treinados para contribuir para a cibersegurança da organização.

Fase 3 - Segurança dos Dispositivos

Nesta terceira etapa, é esperada que seja feita a implementação dos desenhos da arquitetura definidos na fase antecedente. São efetuadas auditorias de segurança e mecanismos de supervisão.

Para que uma organização possa atingir os objetivos propostos é recomendado que sejam implementadas as seguintes ações:

- **A 3.1 –** Definição de procedimentos de operação

- **A 3.2 –** Instalação e configuração de sensores em dispositivos
- **A 3.3 –** Auditoria de segurança e Bases de Dados
- **A 3.4 –** Instalação e configuração de controlo de acessos web – (e.g. serviços
- proxy)
- **A 3.5 –** Proteção e gestão de equipamentos
- **A 3.6 –** Instalação e configuração de mecanismos de monitorização
- **A 3.7 –** Hardening das configurações
- **A 3.8 –** Instalação e configuração de um Security Information and Event
- Management (SIEM)
- **A 3.9 –** Definição de planos de continuidade de negócio
- **A 3.10 –** Aquisição de competências técnicas

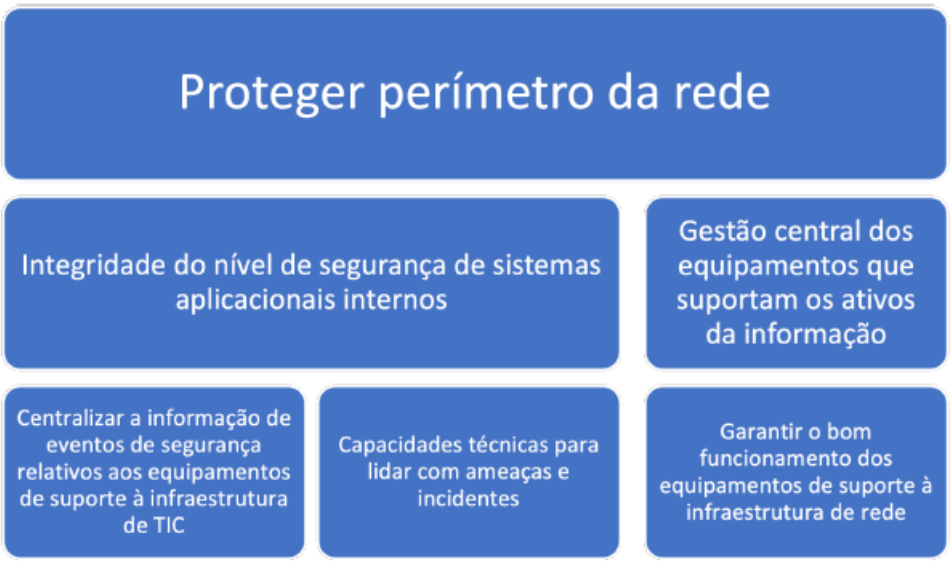

Figura 9-Objetivos para a Fase 3 [14]

Seguidamente serão aprofundados os objetivos:

- **Proteção do Perímetro da Rede:** Implementar dispositivos que filtrem o tráfego com base em políticas definidas, bem como reconheçam e bloqueiem padrões de ataque.
- Garantir a Integridade dos Sistemas Aplicacionais Internos: Realizar auditorias e configurar equipamentos para assegurar a integridade dos sistemas aplicacionais internos.

- **Gestão Centralizada dos Equipamentos que Suportam Ativos de Informação:** Dispor de sistemas que detetem e bloqueiem intrusões, como sistemas HIDS (Host-Based Intrusion Detection Systems) e soluções antivírus.
- **Centralização da Informação de Eventos de Segurança:** Recomenda-se que a organização faça uma gestão eficaz dos eventos de segurança, especialmente por meio de um sistema SIEM (Security Information and Event Management), para filtrar e organizar dados de segurança, tornando as informações mais legíveis e permitindo a tomada de medidas para combater incidentes.
- **Desenvolver Capacidades Técnicas para Lidar com Ameaças e Incidentes:** A organização deve contratar recursos humanos qualificados e implementar sistemas com as capacidades técnicas necessárias para lidar com ameaças e incidentes de cibersegurança.
- **Garantir o Bom Funcionamento dos Equipamentos de Suporte à Infraestrutura de Rede:** Para assegurar o funcionamento eficaz desses equipamentos críticos, é essencial estabelecer mecanismos de monitorização, supervisão e alarme.

Estas ações visam fortalecer a segurança da infraestrutura de TI em múltiplos níveis, abrangendo desde a proteção do tráfego de rede até a capacidade de resposta a incidentes de segurança. Garantir o funcionamento eficiente dos sistemas é fundamental para proteger os ativos e as informações críticas da organização.

Fase 4 - Consolidar a Cibersegurança

Neste momento, é o culminar do processo de capacitação interna no domínio da cibersegurança. De imediato irão ser consolidados e formalizados os processos estabelecidos nas fases prévias. É também estabelecida a gestão de processos de mudança.

As ações necessárias para se atingir o nível máximo desta quarta fase são os seguintes:

- **A 4.1 –** Cadeia de responsabilidades: formalização
- **A 4.2 –** Definição do Sistema Interno de Normas e Políticas (SINP)
- **A 4.3 –** Análise de risco - reavaliação
- **A 4.4 –** Simulacro
- **A 4.5 –** Definição de procedimentos de reação a incidentes
- **A 4.6 –** Treino e sensibilização interna: SINP

- **A 4.7 –** Testes de aceitação de serviços
- **A 4.8 –** Mecanismos de engodo (honeypots)
- **A 4.9 –** Gestão de mudanças e atualizações

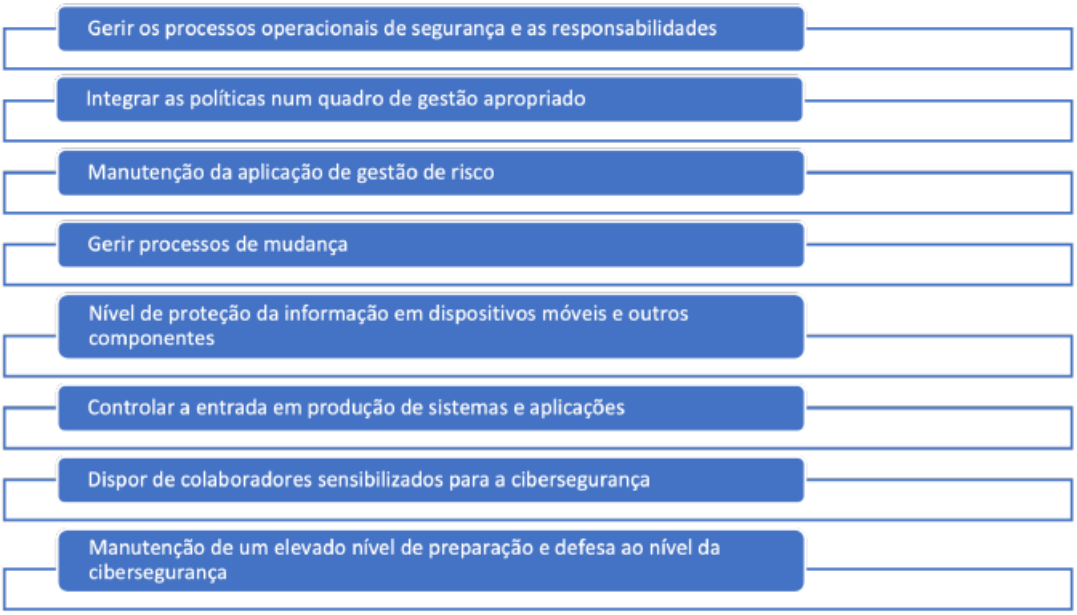

Figura 10- Objetivos para a Fase 4 [14]

Seguidamente serão aprofundados os objetivos desta fase.

- **Gestão dos Processos Operacionais de Segurança e das Responsabilidades:** Estabelecer cadeias de responsabilidades para gerir os processos operacionais, atribuindo responsabilidades específicas para processos e ativos de informação internos.
- **Integração de Políticas num Quadro de Gestão Adequado:** Agregar políticas e normativos definidos nas fases anteriores num quadro de gestão apropriado.
- **Manutenção da Aplicação de Gestão de Risco:** Garantir a manutenção contínua da aplicação de gestão de risco, assegurando que os processos de avaliação de risco são mantidos atualizados.
- **Gestão de Processos de Mudança:** Gerir processos de mudança, como a aplicação de patches e atualizações de segurança, para garantir a compatibilidade dessas alterações com o bom funcionamento dos sistemas aplicacionais e manter um alto nível de proteção dos ativos.

- **Segurança de Dispositivos Móveis e Outros Componentes em Rede:** Considerar a segurança de dispositivos móveis e outros componentes em rede para garantir um alto nível de segurança.
- **Controlar a Entrada em Produção de Sistemas e Aplicações:** Permitir a entrada em produção de sistemas e aplicações somente após testes de segurança e aprovação por parte de uma equipa especializada.
- **Sensibilização de Colaboradores para a Cibersegurança:** Garantir que todos os colaboradores, independentemente das suas funções, estejam sensibilizados para a cibersegurança e apliquem boas práticas nas suas atividades diárias.
- **Manutenção de um Elevado Nível de Preparação e Defesa em Cibersegurança:** Destacar a importância de manter um elevado nível de preparação e defesa em cibersegurança, assegurando a manutenção e melhoria contínua dos sistemas e práticas de segurança.

Estas ações visam fortalecer a capacidade da organização de gerir riscos, responder a ameaças e garantir um alto nível de preparação e defesa em cibersegurança. Ao envolver todos os colaboradores na promoção da cibersegurança, a organização está mais bem preparada para enfrentar os desafios dessa área em constante evolução.

Fase 5 - Equipa de Cibersegurança

Esta etapa aplica-se a organizações cuja dimensão, criticidade/complexidade justifique a criação de um SOC ou CSIRT. A execução desta fase deve ser objeto de avaliação entre a organização e o CNCS.

- **A 5.1 –** Nomear um CISO
- **A 5.2 –** Estabelecer um serviço de gestão de vulnerabilidades
- **A 5.3 –** Estabelecer e implementar um plano de auditorias
- **A 5.4 –** Definir a missão, a comunidade servida e o portfólio de serviços do CSIRT
- **A 5.5 –** Elaborar e fazer aprovar o plano e o orçamento para o CSIRT
- **A 5.6 –** Montar e anunciar o CSIRT
- **A 5.7 –** Estabelecer um sistema de gestão de Crise
- **A 5.8 –** Afiliação nas comunidades nacionais e internacionais de CSIRT
- **A 5.9 –** Participação num exercício nacional de cibersegurança

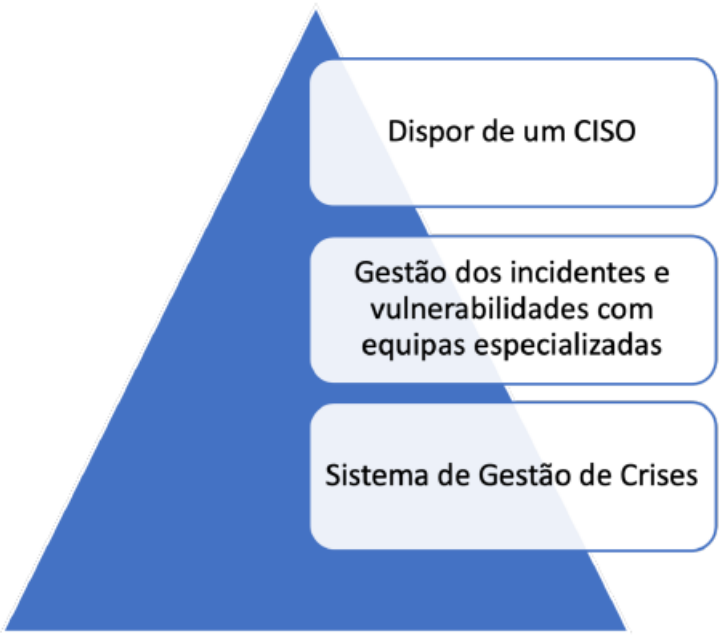

Figura 11- Objetivos para a Fase 5 [14]

Seguidamente vão ser aprofundados os objetivos para esta fase.

- **Nomeação de um Chief Information Security Officer (CISO):** Designar um CISO, que é o responsável máximo pela segurança da informação. Essa figura tem a função de liderar o esforço de cibersegurança e supervisionar as equipas de deteção e resposta a incidentes.
- **Gestão de Incidentes e Vulnerabilidades com Equipas Especializadas:** Contar com equipas especializadas, como o Security Operations Center (SOC) ou o Computer Security Incident Response Team (CSIRT), responsáveis por gerir incidentes e vulnerabilidades de forma eficaz.
- **Implementação de um Sistema de Gestão de Crises:** Implementar um sistema de gestão de crises para reduzir o tempo de reação e aumentar a eficácia no combate a incidentes de cibersegurança de grande magnitude, capazes de causar impactos catastróficos na organização.

Estas ações visam fortalecer a capacidade da organização de detetar, responder e mitigar ameaças de cibersegurança de maneira eficaz. A nomeação de um CISO e o estabelecimento de equipas especializadas são passos críticos para garantir que a organização esteja bem

preparada para lidar com incidentes cibernéticos. Além disso, um sistema de gestão de crises é essencial para garantir uma resposta adequada a incidentes graves.

2.8. Quadro Nacional de Referência para a Cibersegurança

Este documento, desenvolvido pelo Centro Nacional de Cibersegurança, serve como complemento ao Roteiro para as Capacidades Mínimas da Cibersegurança. Este documento disponibiliza medidas de segurança que se traduzem em exemplos e orientações para a cibersegurança. Ao contrário do Roteiro das Capacidades Mínimas não se trata de um conjunto de controlos de ações a realizar. Este contém 103 medidas que correspondem a 5 objetivos de segurança, e que, correspondem a 3 níveis de capacidade.

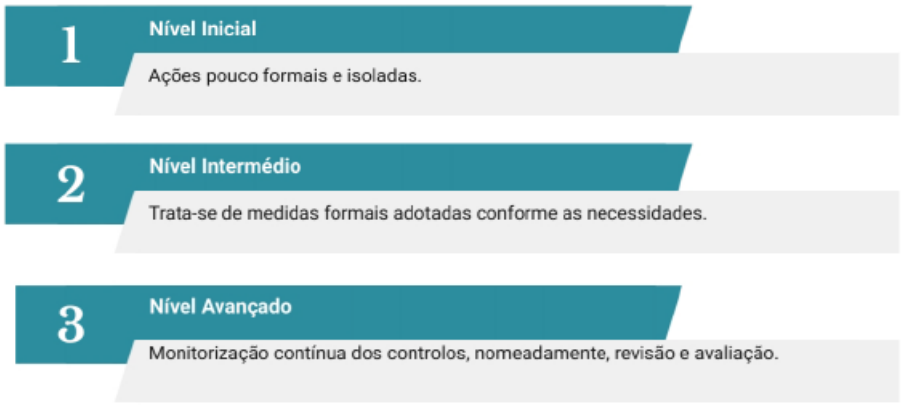

Figura 12- Níveis de Capacidade [15]

No documento referenciado [15] , são apresentadas uma série de diretrizes de boas práticas com o propósito principal de mitigar os riscos relacionados com ameaças enfrentadas pelas organizações. Essas boas práticas formam um conjunto que possibilita que qualquer organização alcance os requisitos mínimos de segurança.

Esses requisitos estão essencialmente focados em cinco objetivos fundamentais, que abrangem a identificação, proteção, deteção, resposta e recuperação em situações de incidentes de segurança. Vale ressaltar que essas orientações são aplicáveis a organizações de variados tamanhos e com diferentes modelos de negócios.

Além disso, o documento QNRCS (Guia de Qualificação Nacional de Referenciação de Cibersegurança) inclui recomendações adicionais que auxiliam as organizações a estar em conformidade com a legislação vigente, ao mesmo tempo em que possibilitam a gestão eficaz de riscos e a minimização do impacto de incidentes.

Figura 13- Objetivos de Segurança [15]

Estes objetivos representados na Figura 13 estão organizados em categorias e subcategorias.

A seguir, apresentam-se os objetivos de segurança, juntamente com breves descrições de cada um deles:

- **Identificar:** Este objetivo concentra-se na identificação dos ativos e serviços críticos da organização, bem como na avaliação dos riscos associados a eles. Isto permite à organização priorizar suas ações de acordo com sua estratégia de gestão de riscos.
- **Proteger:** Neste objetivo, são adotadas as medidas necessárias para proteger os serviços críticos e ativos previamente identificados. Este processo abrange três dimensões: Pessoas, Processos e Tecnologia.
- **Detetar:** Aqui, são definidas e implementadas medidas para detetar incidentes de segurança antecipadamente, permitindo uma resposta mais rápida e eficaz.
- **Responder:** Este objetivo trata da definição e implementação de medidas para responder a incidentes assim que são detetados, com o intuito de mitigar seus impactos.

- **Recuperar:** Envolve a definição e implementação de medidas para recuperar após um incidente de segurança, visando restaurar a normalidade operacional.

É importante ressaltar que este documento não deve ser considerado uma norma por si só, mas sim como uma referência que auxilia na identificação das normas, padrões e boas práticas existentes em diversos domínios da segurança da informação. As medidas de segurança delineadas neste documento podem ser diretamente relacionadas com várias normas. Além disso, o documento também descreve a função de um CISO (Chief Information Security Officer), que desempenha um papel significativo na organização no contexto da segurança da informação.

2.9. Regulamento Geral de Proteção de Dados

Cada vez mais, os dados assumem um valor de grande relevância, o que torna a sua proteção e a manutenção da integridade da informação uma preocupação crescente. Atualmente, os dados são considerados o recurso mais valioso de uma organização e podem ser determinantes para o sucesso ou fracasso dela.

Em abril de 2016, o Parlamento Europeu reconheceu a necessidade de substituir a Diretiva 95/46/CE, que até então regulamentava a proteção de dados. Para abordar a salvaguarda da informação, foi adotado o Regulamento Geral de Proteção de Dados (RGPD) [16] . Este regulamento trouxe um equilíbrio às normas de segurança da informação.

O principal objetivo do RGPD foi estabelecer regras claras em relação à privacidade e à segurança dos dados pessoais. A implementação deste regulamento exigiu que as organizações redefinissem os seus processos para garantir a segurança da informação.

O RGPD baseia-se em dois conceitos-chave:

- **O titular dos dados pessoais deve ter controlo total sobre esses dados.**
- **Simplificação do tratamento de dados pessoais.**

No entanto, apesar da importância dos dados, o seu valor é realçado apenas quando são devidamente tratados e analisados. Portanto, a gestão eficaz dos dados requer a supervisão de um profissional com formação para desenvolver tal função.

De acordo com este regulamento, é esperado que exista um responsável pelo tratamento dos dados para garantir que o processo esteja em conformidade com as suas diretrizes. Este responsável é chamado de Data Protection Officer (DPO). O DPO deve estar presente nas organizações que lidam com grandes volumes de dados e tem a responsabilidade de informar e aconselhar a organização sobre a conformidade com as regulamentações de proteção de dados. Além disso, ele desempenha um papel crucial na formação de outros colaboradores envolvidos nessa área e atua como elo de ligação com as autoridades de proteção de dados.

Figura 14- Etapas para implementação do RGPD [16]

Estão representadas as 8 etapas necessárias para implementar o RGPD na Figura 15.

No que diz respeito aos dados armazenados em bases de dados, é necessário implementar uma camada adicional de segurança. Desta forma, dependendo da natureza dos dados

pessoais e também a sua finalidade, tem de ser garantida a confidencialidade, integridade, disponibilidade e resiliência contínua dos sistemas que tratam os dados.

Este regulamento tornou-se mandatário em Portugal a partir de 25 de maio de 2018.

2.10. Lei nº 46/2018 Regime Jurídico da Segurança do Ciberespaço

Esta legislação é uma resposta direta à Diretiva 2016/1148 da União Europeia, adotada pelo Parlamento Europeu e pelo Conselho em julho de 2016 [17] . Ela foi estabelecida para implementar e incorporar diversos requisitos contidos na mencionada diretiva. Em Portugal, entrou em vigor em 13 de agosto de 2018.

O objetivo fundamental deste regime é garantir um elevado padrão de segurança consistente nas redes e sistemas em toda a União Europeia. Ao adotar este regime, as organizações passam a ter a obrigação de cumprir as disposições estabelecidas para garantir essa segurança.

Entidades abrangidas por este regime
Administração Pública
Operadores de infraestruturas críticas
Prestadores de serviços essenciais
Prestadores de serviços digitais

Tabela 1- Entidades abrangidas por este regime

As entidades mencionadas na Tabela 2 estão obrigadas a aderir a este regime e, da mesma forma, a observar as responsabilidades associadas. Estas responsabilidades incluem:

- **Cumprir os requisitos de segurança estabelecidos na lei**
- **Notificar o Centro Nacional de Cibersegurança em caso de incidente com grande impacto**
- **Informar o Centro Nacional de Cibersegurança qual o seu ramo de negócio**

2.11. Decreto-Lei n.º 65/2021

A lei da segurança do ciberespaço [83] aplica-se a todas as organizações que usem redes e sistemas de informação.

Esta lei pretende regulamentar os requisitos de segurança das redes e sistemas de informação, bem como as regras de comunicação de incidentes.

Os requisitos presentes nesta lei devem ser cumpridos pela administração pública, em geral operadores de estruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais.

Este documento pode-se separar em 8 fases distintas. Estas fases são as seguintes:

• Fase 1: Formação inicial e identificação de catálogos da CIM-TTM

e Associações de Municípios;

• Fase 2: Inventário de Ativos;

• Fase 3: Elaboração de um Plano de Segurança das entidades envolvidas;

• Fase 4: Avaliação intermédia e plano de melhoria;

• Fase 5: Notificação de incidentes;

• Fase 6: Análise de riscos de ativos;

2.2 normas, leis e boas práticas da cibersegurança

• Fase 7: Medidas técnicas para monitorização;

• Fase 8: Revisão do Plano de Segurança.

A lei de cibersegurança [18] é aplicável a todas as organizações que utilizem redes e sistemas de informação. O objetivo desta lei é estabelecer regulamentos para os requisitos de segurança relacionados com redes e sistemas de informação, bem como regras para a notificação de incidentes.

Os requisitos delineados nesta lei devem ser seguidos pela administração pública, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais. Este documento pode ser dividido em oito fases distintas, que são as seguintes:

- **Fase 1:** Formação inicial e identificação de catálogos da CIM-TTM

e Associações de Municípios;

- **Fase 2:** Inventário de Ativos;
- **Fase 3:** Elaboração de um Plano de Segurança das entidades envolvidas;
- **Fase 4:** Avaliação intermédia e plano de melhoria;
- **Fase 5:** Notificação de incidentes;
- **Fase 6:** Análise de riscos de ativos;
- **Fase 7:** Medidas técnicas para monitorização;
- **Fase 8:** Revisão do Plano de Segurança.

2.12. Ameaças a instituições Nacionais

Recentemente, temos testemunhado um aumento significativo nos ataques cibernéticos em território nacional, direcionados a uma ampla gama de organizações. Estes ataques têm objetivos variados, resultando em diversos tipos de impacto, dependendo do alvo escolhido.

Em janeiro de 2022 o grupo Impresa sofreu um ataque de sabotagem e destruição, eliminando permanentemente dados e arquivo de televisão e interrompendo seriamente os serviços de informação.

Em fevereiro de 2022 a Vodafone também sofre um ataque de sabotagem e destruição de tal ordem que as redes, móvel e fixa ficaram offline por algum tempo. Demorou mais de uma semana a recuperar a informação e a operacionalidade completa da rede.

Ainda em fevereiro de 2022, os laboratórios da Germano de Sousa foram alvo de um ataque informático de encriptação de dados com o objetivo de pedir um resgate (ransomware). Houve um bloqueio nos serviços administrativos, provocando elevados atrasos a nível de agendamentos dos exames.

Em abril de 2022, o hospital Garcia da Horta sofreu um ataque informático de encriptação de dados com o objetivo de pedir um resgate (ransomware), provocando um grande atraso nos agendamentos por bloqueio dos serviços administrativos.

Em setembro de 2022 A TAP Air Portugal sofreu um ataque por encriptação de dados com o objetivo de pedir resgate (ransomeware). Foi divulgada informação de dados pessoais dos clientes.

Em outubro de 2022, a Universidade da Beira Interior foi alvo de um ataque informático que levou à encriptação de dados com o objetivo de pedir resgate. Vários serviços foram afetados. Demorou várias semanas até à reposição dos sistemas.

Em novembro de 2022 o Instituto de Segurança Social foi alvo de ataque por sabotagem e destruição, tornando o serviço indisponível por algum tempo.

Em maio de 2023 o Sistema informático da Câmara de Lagoa foi alvo de ataque informático. Além da transferência de uma quantidade considerável de informação, foram encriptados vários ficheiros. Devido ao sistema de redundância que estava implementado na autarquia, com cópias quase diárias para um servidor, foi possível recuperar quase a totalidades dos dados perdidos.

Em agosto de 2023 o Serviço Regional de Saúde da Madeira (Sesaram) sofreu um ataque informático de sabotagem, tornando indisponível os serviços por algum tempo. Não foi pedido nenhum resgate.

3.Cibersegurança na área do IOT

O avanço tecnológico rápido e constante tem conduzido ao desenvolvimento de novas técnicas e produtos destinados a aprimorar a qualidade de vida das pessoas. Na área da saúde, tem havido um aumento significativo de equipamentos de diagnóstico e tratamento menos invasivos e mais seguros, com o objetivo de melhorar a qualidade de vida e promover a longevidade.

Para atender à crescente demanda por viver mais e com melhor qualidade, minimizando o sofrimento, a tecnologia tem se aliado à inovação e a várias disciplinas, incluindo robótica, radiologia, bioquímica, biofísica, electromedicina, informática e muito mais.

O termo "Internet das Coisas" (IoT) [19] é uma denominação ampla que se refere aos esforços em curso para conectar uma ampla variedade de dispositivos físicos às redes de comunicação. Atualmente, não se limita apenas a computadores, abrangendo uma ampla gama de dispositivos conectados à Internet, como TVs, refrigeradores, eletrodomésticos, veículos, smartphones, câmaras de vigilância, fechaduras inteligentes, sensores e muito mais.

O termo Healthcare 4.0 [20] está relacionado com a indústria 4.0 que abrange as tecnologias emergentes que ajudam a otimização de tomadas de decisões estratégicas e inteligentes entre elas, seja o IoT, o big data, a computação na cloud, a gestão analítica e a inteligência artificial.

De acordo com uma pesquisa do Ponenon Institute [20] , revelou-se que 39% dos fabricantes de equipamentos médicos admitiram que indivíduos maliciosos conseguiram assumir o controlo de um desses dispositivos, e apenas 15% das organizações de cuidados de saúde confirmaram a adoção de medidas significativas para prevenir esses ataques. Além disso, em março de 2019, o Departamento de Segurança Interna dos Estados Unidos emitiu um alerta para pacientes com desfibriladores cardíacos, destacando o risco de cibercriminosos assumirem o controlo remoto desses dispositivos, colocando em perigo a vida de milhões de pessoas. Esses incidentes estão frequentemente relacionados com a falta de autenticação e a ausência de criptografia.

Na área da saúde, a Internet das Coisas (IoT) desempenha um papel cada vez mais importante, contribuindo para a eficiência dos hospitais e unidades de saúde. Isto é evidente na monitorização de pacientes em ambiente domiciliário, na monitorização cardíaca com alarmes, na utilização de sensores e programas terapêuticos que monitorizam a atividade cerebral dos pacientes e em muitos outros cenários.

Nos ambientes hospitalares, uma variedade de sistemas e dispositivos conectados à Internet ou à rede são utilizados, incluindo bombas de insulina, pacemaker, dispensadores de medicamentos, estações de aquisição de imagem, UPS (uninterruptible power supply), impressoras, controladores autómatos (responsável, por exemplo, para o quadro geral de baixa tensão - QGBT), câmaras de vigilância, sistemas de controlo de acesso (biométricos, cartões de proximidade RFID), as pulseiras anti rapto, quiosques de pagamento automático, central telefónica, os aparelhos de picking, entre outros.

Embora esses dispositivos IoT desempenhem um papel vital nas operações diárias de saúde, eles também apresentam riscos significativos. A transformação digital na área da saúde trouxe melhorias nos procedimentos de diagnóstico e monitorização, reduzindo os custos dos cuidados de saúde. No entanto, a proliferação destes dispositivos aumenta a exposição a ameaças de segurança e privacidade. Para enfrentar este desafio, é essencial realizar uma inventariação precisa dos dispositivos conectados à rede e implementar medidas de segurança rigorosas.

A correta inventariação dos dispositivos na rede é crucial, e existem aplicações e programas que podem ajudar nesse processo, como OpenVas, Nessus, Nexpose, Secapps, W3af, Wapiti, WebReaver, DVCS Ripper e Arachni. No entanto, é importante notar que estas aplicações podem não identificar de forma precisa todos os dispositivos, levando a possíveis falsos positivos antes da sua catalogação.

Portanto, as equipas de tecnologia da informação nas instituições de saúde devem realizar uma inventariação completa e monitorização constante dos dispositivos na rede, garantindo que as atualizações de segurança sejam aplicadas quando necessário. A Associação Americana de Hospitais [24] reconhece que os dispositivos médicos conectados à Internet oferecem melhorias significativas no atendimento ao paciente e na eficiência, mas também destacam a necessidade crítica de identificar riscos e vulnerabilidades para evitar incidentes que possam colocar vidas em risco.

3.1. Tipos de Comunicação

Os protocolos de rede e os tipos de comunicação tem evoluído e aparecido no mercado à medida que os equipamentos IoT surgem e amadurecem. As taxas de transferência, ou número de nós que permite ligar em simultâneo, assim como da distância do gateway, estão na origem de novos e variados tipos de comunicação.

Os diversos dispositivos que formam os equipamentos IoT são limitados ao nível de recursos, no entanto a sua forma de comunicação é muito heterogénea e a forma como comunicam difere de equipamento para equipamento.

Os métodos para recolha de informação têm evoluído conforme as formas de comunicação ganham maturidade, aumentando assim a utilização e a proliferação de equipamentos ligados à internet.

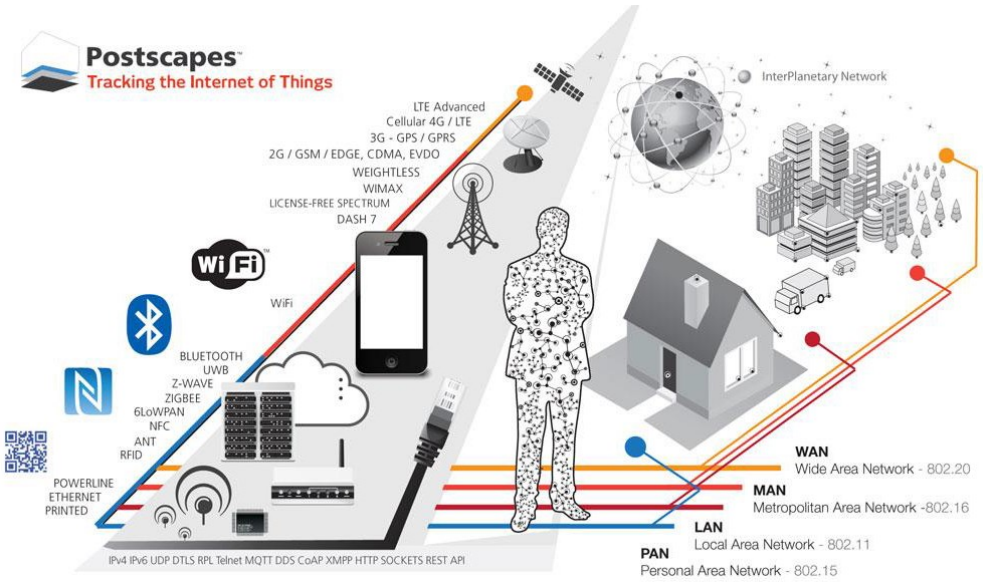

Figura 15 - Diagrama de conectividade

A figura 2 apresenta as diversas formas de transmitir a informação recolhida, tais como o wi-fi, o Bluetooth, o NFC, entre outros, bem como o espectro de alcance dessa informação, passando das redes pessoais (PAN), onde se considera a utilização de um monitor cardíaco, ou um dispositivo móvel, redes locais (LAN), redes metropolitas (MAN) ou redes de longa distância (WAN). Esta figura demonstra também como o IoT se vem enraizando na nossa sociedade, evidenciando a ideia cada vez mais adotada de que a informação pode ser proveniente de qualquer "coisa".

Como se pode constatar é notável a crescente evolução das mais variadas tecnologias pelo que se tem verificado que estas têm acompanhado as necessidades dos variados negócios onde se enquadram. Os fabricantes têm tentado responder às solicitações que lhes são pedidas, pelo que diariamente aparecem novos produtos com novas funcionalidades e vários propósitos.

Na figura 3 está presente a evolução dos demais protocolos ao longo dos anos. Durante este período o âmbito de ação também foi alargado, assim como existiu um crescimento e o aparecimento de novos sistemas e funcionalidades.

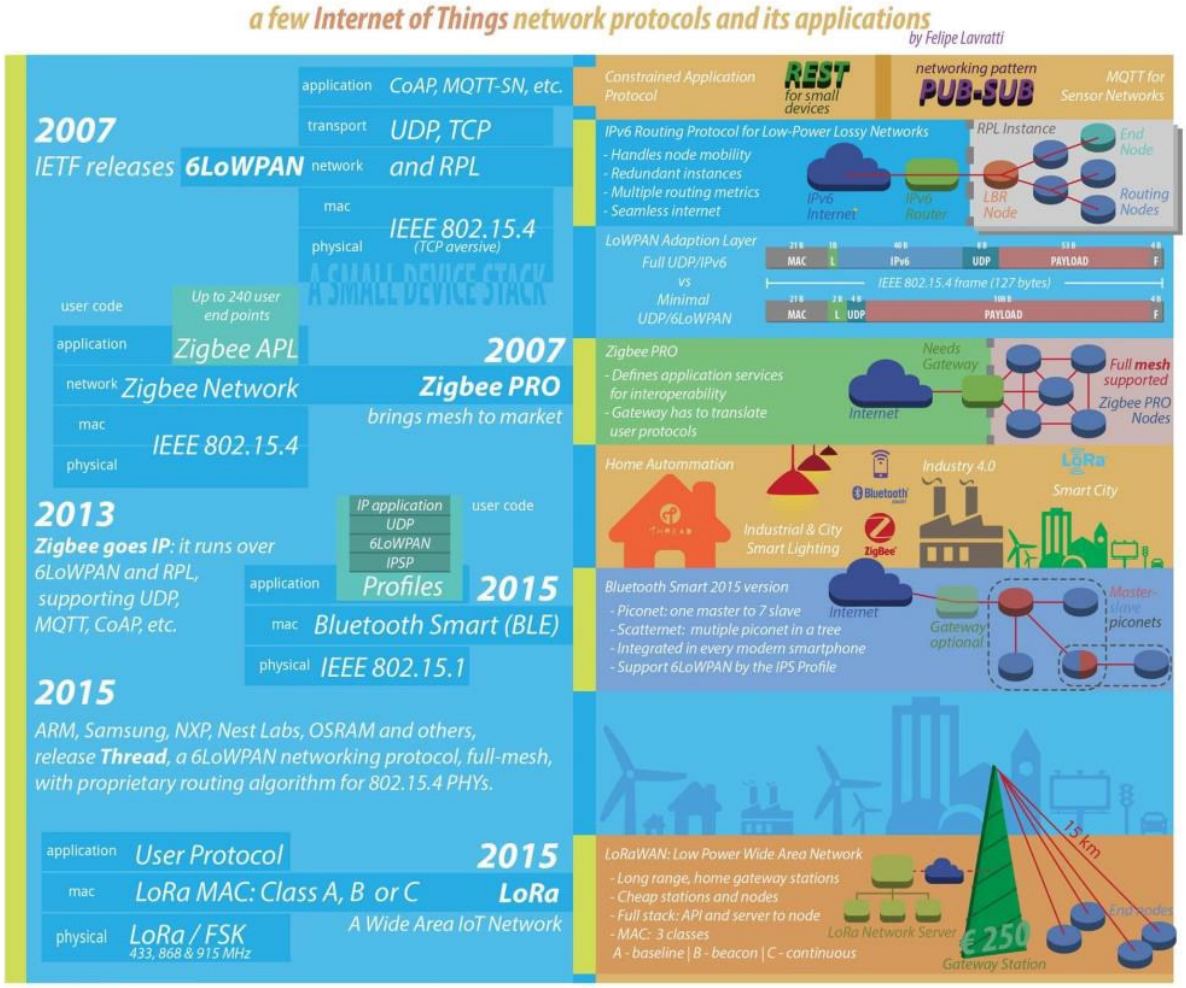

Figura 16- Protocolos de rede IoT e sua aplicação

Atualmente existe a necessidade de se estar ligado ao mundo, de ver mais alem e as demais tecnologias têm acompanhado essas espectativas e dado resposta aos utilizadores.

Com o rápido desenvolvimento das Internet das Coisas, a monitorização da saúde tem adquirido novos players no mercado, contudo a introdução destes novos equipamentos tem trazido novos desafios, sendo que uma das principais preocupações se foca nos protocolos de comunicação [25] .

Elencam-se assim os principais tipos de comunicação de equipamentos IoT ao longo dos anos:

3.1.1. 6LowPAN

O protocolo 6LowPan [26] [27] é um protocolo IP (Internet Protocol) cujo nome é uma abreviação de IPv6 Low-power wireless Personal Area Network. Apesar de ser uma

tecnologia IoT, assim como o Bluetooth ou o ZigBee, o 6LowPan é um protocolo de rede que define o encapsulamento, cabeçalhos e utiliza mecanismos de compressão. A característica fundamental é a inclusão da pilha IPv6, o que representa um passo significativo para tornar a Internet das Coisas uma realidade. Com o IPv6, torna-se possível atribuir um endereço IP único a cada objeto ou dispositivo em todo o mundo, permitindo sua conexão à rede e à internet.

Esse tipo de comunicação [28] remove alguns cabeçalhos do IPv6 e UDP, pois eles geralmente possuem valores conhecidos. Nas aplicações mais comuns das redes de sensores, apenas um número limitado de portas é utilizado, tornando quatro bits suficientes para sua descrição, em vez dos tradicionais 8 bits.

3.1.2. ZigBee

O Zigbee [29] é um dos protocolos mais amplamente utilizados, com aplicações predominantemente voltadas para ambientes industriais em vez de residenciais. Ele baseia-se no padrão IEEE 802.15.4, que é um padrão para redes sem fio operando na faixa de 2.4GHz. As aplicações Zigbee geralmente não exigem mudanças frequentes na taxa de transmissão. Todos os principais fabricantes de semicondutores incluem módulos Zigbee nos seus portfólios de produtos. O alcance deste protocolo varia de 10 a 100 metros, e a taxa de transmissão atinge um máximo de 250 kbps. Atualmente, a manutenção deste protocolo é de responsabilidade da empresa Zigbee Alliance.

3.1.3. Bluethooth

O protocolo está sob a alçada da empresa Bluetooth SIG (Special Interest Group) [30] , e é caracterizado por possuir uma vasta documentação e uma abundância de exemplos de aplicações disponíveis na internet. Este fator torna a integração desta tecnologia em projetos de automação residencial, comercial e produtos eletrónicos de forma consideravelmente mais fácil. O alcance do protocolo varia de acordo com a classe do módulo. Os chips da Classe 1 conseguem abranger distâncias de até 100 metros, com uma potência de 100 mW. Já os módulos da Classe 2 têm um alcance de até 10 metros e uma potência de 2,5mW. A Classe 3, por sua vez, possui um alcance limitado de apenas 1 metro e consome no máximo 1 mW.

Relativamente ao Bluetooth 5.0, este consegue alcançar distâncias de até 240 metros, com uma taxa de transmissão de 50 Mbit/s.

Quando os dispositivos se encontram dentro do raio de alcance, eles podem ser localizados independentemente da sua localização específica, o que permite que funcionem em ambientes diferentes, com base na potência do dispositivo.

3.1.4. Wi-Fi

As redes Wi-Fi operam conforme o padrão IEEE 802.11.b, g,n [31] , que abrange as frequências de 2.4 GHz e 5 GHz, e empregam sinais de Radio Frequência (RF) para transmissão. São reconhecidas pela sua qualidade e flexibilidade, sendo particularmente adequadas para uso a distâncias moderadas, abrangendo dezenas de metros. Esta tecnologia experimentou uma evolução significativa em termos de taxas de comunicação, atingindo velocidades de transmissão muito elevadas (na ordem de Gbps).

Este tipo de comunicação possibilita a transferência de dados para uma ampla gama de dispositivos, incluindo computadores, laptops, smartphones, tablets e outros aparelhos compatíveis com esta tecnologia, tudo de forma simultânea. Além disso, proporciona uma liberdade de uso significativa, uma vez que não se limita a uma área específica, devido ao seu alcance considerável.

3.1.5. RFID

O RFID - Identificação por Radiofrequência (Radio-Frequency IDentification) [32] utiliza campos magnéticos para realizar a identificação e o rastreamento automático de etiquetas, também conhecidas como "tags", que são afixadas em objetos. Os sistemas RFID compreendem dispositivos eletrónicos chamados de "transponders" ou "tags", que interagem com leitores designados para essa finalidade. As tags RFID possuem antenas que permitem receber e responder a solicitações por radiofrequência, dispensando a necessidade de alimentação elétrica para funcionar. A frequência de operação varia de 100 KHz a 5,8 GHz, e o alcance efetivo depende do leitor, podendo atingir até 8 metros.

3.1.6. NFC

A Near Field Communication (NFC) [33] é uma tecnologia empregada para a troca de informações entre dois dispositivos eletrónicos. Ela é uma extensão da tecnologia de cartões RF (RFID) que possibilita a comunicação entre dispositivos numadistância muito curta, geralmente de apenas alguns centímetros. As taxas de transmissão variam de 100 a 420 kbps. O padrão NFC é definido pela norma ISO/IEC 18000-3. Essa tecnologia permite a transferência de dados entre dispositivos sem a necessidade de cabos, porém, requer que os dispositivos estejam fisicamente próximos, já que o alcance típico desse protocolo é de apenas 10 cm.

3.1.7. Thread

Foi lançado em 2014 pelo Thread Group [34] e é baseado em vários padrões, incluindo o IEEE802.15.4, IPv6 e 6LoWPAN. Oferece uma solução do tipo IP para IoT em âmbito residencial. Este tipo de comunicação possibilita gerir uma rede com até 250 nós.

3.1.8. LoRaWAN

O protocolo LoRa [35] foi depassworddo para comunicações de baixo consumo energético. Mantido pela LoRa Alliance, este protocolo suporta redes amplas com milhões de equipamentos e possui velocidade entre 0.3 kbps até 50 kpbs. É um dos protocolos IoT mais populares.

A seguinte tabela apresenta uma comparação dos diversos tipos de comunicação utilizados pelos equipamentos IoT, relativamente á frequência, ao alcance, à autonomia, tipologia e nós:

Tecnologia	Standard	Rate/ Frequency	POWER	Alcance	Bateria	Tipologia	Nós
WI-FI	IEEE 802.11b	54 Mbps	400/ 20 mA	1-100m	Horas	Estrela	64+190
RFID	ISO/IEC 18000	125Khz, 13,56Mhz 800Mhz a 960Mhz 2,45Ghz ou 5,8Ghz	-	Metros	-	Estrela	7
ZIGBEE	IEEE 802.15.4	20 to 250 Kbps	30mA/ 356uA	100+m	Meses/ Anos	STAR	32
BLUETOOTH	IEEE 802.15.1	1 Mbps	49mA/ 0,2mA	1-10 m	Dias	P2P/STAR	254 A 64516
NFC	ISO/IEC 18092	424 Kbps	-	1-10 cm	Meses/ Anos	1 + 1	2
6LowPAN	IEEE 802.15.4	868-868.6 MHz 902-928 MHz 2400-2483.5 MHz		10 a 100m	Anos	Estrela / Malha	
Thread	IEEE 802.15.4	2.4GHz	400 mA	10 cm		Estrela	250
LoRaWAN	IEEE 802.11ah	109 MHz, 433 MHz, 866 MHz e 915 MHz		2km a 45km		Estrela	

Tabela 2 - Comparação dos Tipos de Comunicação [36]

3.2. Protocolos de comunicação

À medida que as tecnologias continuam a evoluir, novos protocolos surgem para atender às necessidades específicas dessas tecnologias. Isto torna as comunicações mais eficientes, transmitindo apenas o essencial com base no propósito para o qual são destinadas. A seguir, são listados os principais protocolos utilizados nas comunicações de dispositivos IoT:

3.2.1. MQTT - Message Queue Telemetry Transport

O protocolo MQTT [37] teve sua origem na década de 90, desenvolvido pela IBM para aplicações de supervisão e aquisição de dados em ambientes industriais, como o SCADA (Supervisory Control and Data Acquisition). Este protocolo adota o modelo de mensagens baseado na publicação e subscrição [38] e foi projetado para operar sobre TCP. Uma das suas principais vantagens é o baixo consumo de recursos, além da sua capacidade de funcionar em redes sujeitas a falhas intermitentes.

3.2.2. CoAP – Constrained Application Protocol

Em junho de 2014, o RFC 7252 [39] introduziu o CoAP [40] como um protocolo de troca de mensagens direcionado a dispositivos com restrições severas de processamento, memória e energia, especialmente projetado para redes com largura de banda limitada. O CoAP utiliza o modelo cliente/servidor e oferece interações unilaterais do tipo 'pedido/resposta'. Uma diferença notável em relação ao MQTT é que o CoAP foi desenvolvido para operar diretamente com o protocolo HTTP. De acordo com [39] , esse protocolo permite a troca de mensagens assíncronas e oferece recursos simples de proxy e cache, suportando métodos como GET, POST, PUT e DELETE, facilitando a obtenção, envio e exclusão de dados entre dispositivos.

3.2.3. HTTP - HyperText Transfer Protocol

O HTTP [41] foi especialmente desenhado para a internet em 1997. O HTTP é um protocolo simples baseado em texto sem tamanho fixo para o cabeçalho. Possui características para ligações persistentes e não persistentes. Por defeito, é utilizado TCP como protocolo de transporte do HTTP.

Trata-se de um protocolo muito poderoso [42] , no entanto utiliza demasiados recursos de rede o que dificulta a sua adoção em equipamentos IoT.

3.3. Normas de comunicação

A definição de normas standard e a padronização das comunicações tem vindo a ser implementada há largos anos. No entanto, sua implementação completa tem sido desafiadora devido ao fato de que cada fornecedor tende a criar o seu próprio mercado. Com a interoperabilidade a ganhar terreno, este tipo de padrão tem ganho cada vez mais adeptos e as aplicações clínicas e os equipamentos médicos começaram a comunicar com os protocolos standard mais comuns nesta área, são eles o HL7, o DICOM e o OpenEHR.

3.3.1. HL7 – Health Level Seven

O Protocolo HL7 é uma plataforma de troca de mensagens entre dispositivos médicos, sistemas de informação e bases de dados clínicas. Ele estabelece um conjunto de regras e formatos que garantem a interpretação das informações, independentemente de sua origem. O HL7[43] é uma estrutura padrão desenvolvida por uma organização sem fins lucrativos chamada Health Level Seven, fundada em 1987 e certificada pelo ANSI (American National Standards Institute) para desenvolver padrões de saúde desde 1994 (Health Level Seven, 2017). Em Portugal, o protocolo HL7 é amplamente usado e reconhecido [44] como uma norma aceita pelo governo, empresas de software e fabricantes de dispositivos médicos, facilitando a troca de dados entre diferentes soluções.

3.3.2. DICOM - Digital Imaging and Communications in Medicine

As normas DICOM [45] padronizaram a transmissão de imagens médicas, garantindo um único formato para todas as modalidades de exame. Isto permite que as imagens sejam visualizadas por dispositivos de diferentes fabricantes. Esta normalização melhorou significativamente a qualidade das imagens, resultando em diagnósticos mais precisos. Além disso, o padrão DICOM permite verificar se uma imagem específica foi gravada ou transmitida com sucesso, garantindo que nenhum arquivo seja perdido durante o processo.

3.3.3. OpenEHR

O openEHR [46] é um conjunto de especificações de código aberto para registos eletrónicos de saúde. Ele tornou-se uma referência internacional para a criação de modelos de conteúdo clínico, com base no padrão ISO 13606. Esta abordagem promove a interoperabilidade das informações clínicas entre diferentes sistemas de saúde. O openEHR propõe uma metodologia de desenvolvimento em dois níveis, abordando tanto o aspeto de software quanto a camada de conhecimento clínico.

3.4. Ataques de Segurança

Os ataques de segurança direcionados a instituições de saúde têm sido uma ocorrência frequente. Um exemplo recente remonta a fevereiro de 2019, quando o Melbourne Heart Group[47] sofreu um ataque de ransomware, no qual os cibercriminosos criptografaram todos os dados nos seus servidores. Outro incidente relevante ocorreu em 2018 envolvendo o sistema de saúde de Singapura, o SingHealth[48] que sofreu uma enorme violação de dados, incluindo os registos de saúde do primeiro-ministro, seguido pelo roubo dos registos de 16 mil pacientes no UnityPoint[49] algumas semanas depois. Em maio de 2017, o ataque WannaCry[50] resultou no cancelamento de mais de 19 mil consultas no Serviço Nacional de Saúde do Reino Unido e em um gasto de mais de 150 milhões de libras na tentativa de remediar a situação.

Devido à grande quantidade de informação pessoal que foi possível roubar e transferir eletronicamente, as organizações de saúde tornaram-se nos principais alvos dos cibercriminosos que, para além de quererem causar disrupção em massa, também pretendem lucrar com o ataque que originam.

Um sistema IoT pode ser alvo de ataques de diversas formas, incluindo ataques físicos, dentro da própria rede ou com o uso de recursos de outros dispositivos. Dado que os dispositivos IoT são implementados em diversas tecnologias de rede, é essencial catalogar adequadamente os tipos de ataques para desenvolver medidas preventivas ou de mitigação apropriadas.

A tabela 2 resume a classificação [51] dos ataques de equipamentos IoT:

Ataques físicos	Ataques de rede	Ataques de software	Ataques de criptografias
Alteração de Nós	Análise de Tráfego	Vírus	Ataque de texto cifrado
Injeção de nó malicioso	Eavesdropping	Spyware	Ataque de código cifrado
Injeção de código malicioso	Message Injection	Adware	Man-in-the-midle
Engenharia Social	Message Replication	Cavalo de Troia	Ransomware
Radio Jamming	Sinkhole Attack	Scripts Maliciosos	
Node Destruction	Sybil Attack	DoS	
Hello Flooding	Message Alteration	Malware	
Black Hole Attack	DoS		
Wormhole Attack	RFID Spoofing		
Slowdown	RFID Cloning		
	Man-in-the-midle		

Tabela 3 - Classificação de Ataques em IoT [52]

3.5. Tipos de Ameaça

Qualquer dispositivo conectado a uma rede está sujeito a ser alvo de ataques, seja por motivos comerciais, destrutivos, vandalismo, terrorismo ou simplesmente para identificar vulnerabilidades nos sistemas, servidores ou dispositivos interconectados. Esta busca por vulnerabilidades tem como objetivo primordial aprimorar a segurança desses dispositivos.

Apesar do grande potencial do IoT em diversas áreas de atuação, a infraestrutura de comunicação dos dispositivos IoT apresenta falhas de segurança conhecidas [53] [54] , tornando-se vulnerável à quebra de privacidade dos dados transmitidos.

De acordo com estudos realizados [55] pela ENISA Threat Taxonomy42 [56] , listamos as principais ameaças:

3.5.1. DoS

Um ataque por DoS [57] , Denial of Service, tem como alvo um sistema IoT, resultando na indisponibilidade e interrupção da produção devido a um grande volume de solicitações enviadas para o sistema. Mesmo com mecanismos de defesa baseados em análise de cookies, conforme descrito no RFC 8576 [58] , os dispositivos IoT podem ser vulneráveis, pois os atacantes geralmente possuem maior capacidade de processamento.

3.5.2. Malware

O malware envolve a inserção de software malicioso, projetado para realizar ações não autorizadas, podendo causar danos ao dispositivo ou à rede. ransomware[1], vírus, cavalos de troia e spyware[2] são exemplos comuns dessa ameaça.

3.5.3. Manipulação de hardware ou software

Essa ameaça concentra-se na manipulação não autorizada de dispositivos, alterando as suas configurações e finalidades previstas. São ataques que alteram o código-fonte do dispositivo, fazendo com que pareça operar normalmente enquanto executa tarefas adicionais, como o envio não autorizado de dados para outro local ou servidor.

3.5.4. Manipulação da informação

A manipulação de informações pode ocorrer quando um invasor intercepta o tráfego de rede e o modifica antes de entregá-lo ao destinatário. Esse tipo de ataque, geralmente chamado de "Man-in-the-Middle," pode ser realizado por meio de malware projetado para esse fim, sendo difícil de detetar pelo utilizador final.

[1] Tipo de software nocivo que restringe o acesso ao sistema infetado encriptando os dados de um sistema e que solicita um resgate em cripto moedas para resgate da informação.

[2] Aplicação que se permanece instalada no sistema operativo para espiar o utilizador, fornecendo informações ao seu autor.

3.5.5. Brute Force

Esse tipo de ameaça visa obter acesso não autorizado a recursos da organização por meio de tentativas repetidas. Começando com credenciais padrão, passando por ataques de dicionário e até mesmo recorrendo a engenharia social para direcionar ataques a utilizadores específicos. Estes ataques são demorados e visam explorar a vulnerabilidade das credenciais.

3.5.6. Ataques direcionados

Os ataques direcionados têm como objetivo roubar informações de alvos específicos. São ataques planeados e estruturados que podem levar dias, meses ou semanas para serem preparados e implementados, visando alcançar resultados desejados.

3.5.7. Reconhecimento de rede

Esta técnica procura validar a conexão de nós na rede, identificar serviços ativos e verificar a presença de vulnerabilidades nas aplicações. O reconhecimento de rede [59] envolve a pesquisa em todos os nós da rede para identificar características detalhadas, como portas e endereços IP.

3.5.8. Man-in-the-Middle

O ataque Man-in-the-Middle ocorre quando um invasor se posiciona no meio da comunicação, interceptando, lendo e até mesmo alterando informações antes de enviá-las ao destinatário. Isso permite que os dados sejam espionados e manipulados sem que os utilizadores percebam.

3.5.9. Vandalismo ou terrorismo

Os dados numa rede de computadores podem ser alvo de vandalismo, causando indisponibilidade ou exigindo resgate financeiro. Esta forma de terrorismo pode prejudicar gravemente o modelo de negócios de uma instituição, resultando em prejuízos significativos.

3.5.10. Sabotagem

A sabotagem visa interromper o funcionamento normal de sistemas, causando indisponibilidade. As formas de sabotagem podem incluir cortes de energia, cortes físicos de cabos, curtos-circuitos induzidos e outros métodos.

3.5.11. Ataques de Botnets

Os ataques de botnets geralmente envolvem cavalos de Troia para violar a segurança do sistema. Estes robots realizam tarefas automaticamente, proporcionando negação de serviço ou acesso não autorizado a informações privilegiadas.

3.5.12. Exploits de vulnerabilidades

Neste tipo de ameaça, o invasor aproveita as falhas de firmware ou software do dispositivo IoT. A falta de atualizações, o uso de passwords por defeito ou configurações inadequadas tornam os dispositivos IoT frequentemente vulneráveis. Bibliotecas atualizadas de vulnerabilidades comuns para diferentes dispositivos IoT facilitam a identificação de falhas e a exploração dessas vulnerabilidades.

3.5.13. Negligência dos funcionários

A negligência dos funcionários é outra ameaça comum nas organizações, devido à falta de cultura de segurança. A partilha de passwords, a ausência de bloqueio de estações de trabalho e a falta de atualização de passwords são exemplos de negligência interna que pode comprometer inadvertidamente a segurança das organizações.

Na seção seguinte, abordaremos alguns tipos de dispositivos IoT comuns em organizações ou unidades de saúde, destacando os riscos e vulnerabilidades associados à utilização inadequada ou sem conformidade, juntamente com exemplos de ataques a que estão sujeitos.

3.6. Riscos dos Equipamentos IoT

O Internet of Things (IoT) oferece uma ampla gama de possibilidades de uso, mas é fundamental estar ciente dos desafios que isso pode apresentar no futuro. Este capítulo concentra-se nos riscos associados aos dispositivos IoT e na necessidade de uma identificação precisa desses riscos.

A identificação de riscos desempenha um papel crucial para entender como e onde agir, visando mitigar ou eliminar qualquer ameaça à segurança ou à privacidade de dados que possa surgir devido ao uso inadequado desses dispositivos.

Os dispositivos IoT conectados à rede na área de saúde [60] representam alvos atraentes para hackers, cibercriminosos e indivíduos mal-intencionados, por várias razões:

- As organizações de saúde possuem inúmeros dispositivos conectados à rede, e algumas dessas unidades podem apresentar lacunas de segurança.
- Os dispositivos IoT pessoais utilizados por pacientes, familiares e funcionários geralmente não passam por avaliações das equipas de tecnologia da informação locais.
- Estes dispositivos armazenam informações valiosas, como dados pessoais e históricos de saúde, que podem ser explorados para fins lucrativos.

O novo paradigma do IoT envolve a integração de objetos e dispositivos nas redes, muitas vezes com baixos custos, e a maioria deles possui capacidade de conexão à internet. No entanto, a capacidade de controlo remoto ou por meio de smartphones varia de dispositivo para dispositivo.

As aplicações de IoT estão em constante expansão, com o surgimento diário de novos aplicações, sensores e funcionalidades. Cada novo desenvolvimento traz consigo desafios de segurança que precisam ser superados para garantir a confiabilidade, integridade e disponibilidade dos dados transmitidos e recolhidos.

De acordo com uma pesquisa publicada pelo HIPAA Journal [61] , 89% dos executivos de saúde relataram violações de segurança relacionadas à adoção de IoT, e 49% identificaram o malware como um problema [62] .

As unidades de saúde enfrentam um desafio único quando se trata de segurança da informação. Estas instituições são um emaranhado de "sistemas de sistemas" com enormes matrizes de equipamentos interligados entre si. Isto cria múltiplos pontos de entrada na rede, tornando a gestão da segurança complexa e criando uma ampla superfície de ataque para cibercriminosos.

De acordo com o Instituto Nacional de Padrões e Tecnologia (NIST) [63] [64] , as ameaças à cibersegurança podem ter um impacto negativo nas redes das organizações de saúde e nos dispositivos IoT conectados a essas redes. Esses impactos podem prejudicar o fluxo de trabalho hospitalar, interromper procedimentos clínicos ou afetar a disponibilidade dos serviços de saúde.

Os dispositivos IoT apresentam um potencial significativo de riscos, e a comunidade "OWASP Internet of Things" [65] desenvolveu um projeto para ajudar fabricantes, desenvolvedores e consumidores a compreender melhor as questões de segurança associadas a esses dispositivos. Essa conscientização é fundamental para tomar decisões mais informadas sobre segurança ao criar, adotar ou implementar soluções de IoT.

Em dezembro de 2018, a OWASP divulgou a lista dos 10 principais riscos de IoT para 2019, apresentando a seguinte imagem:

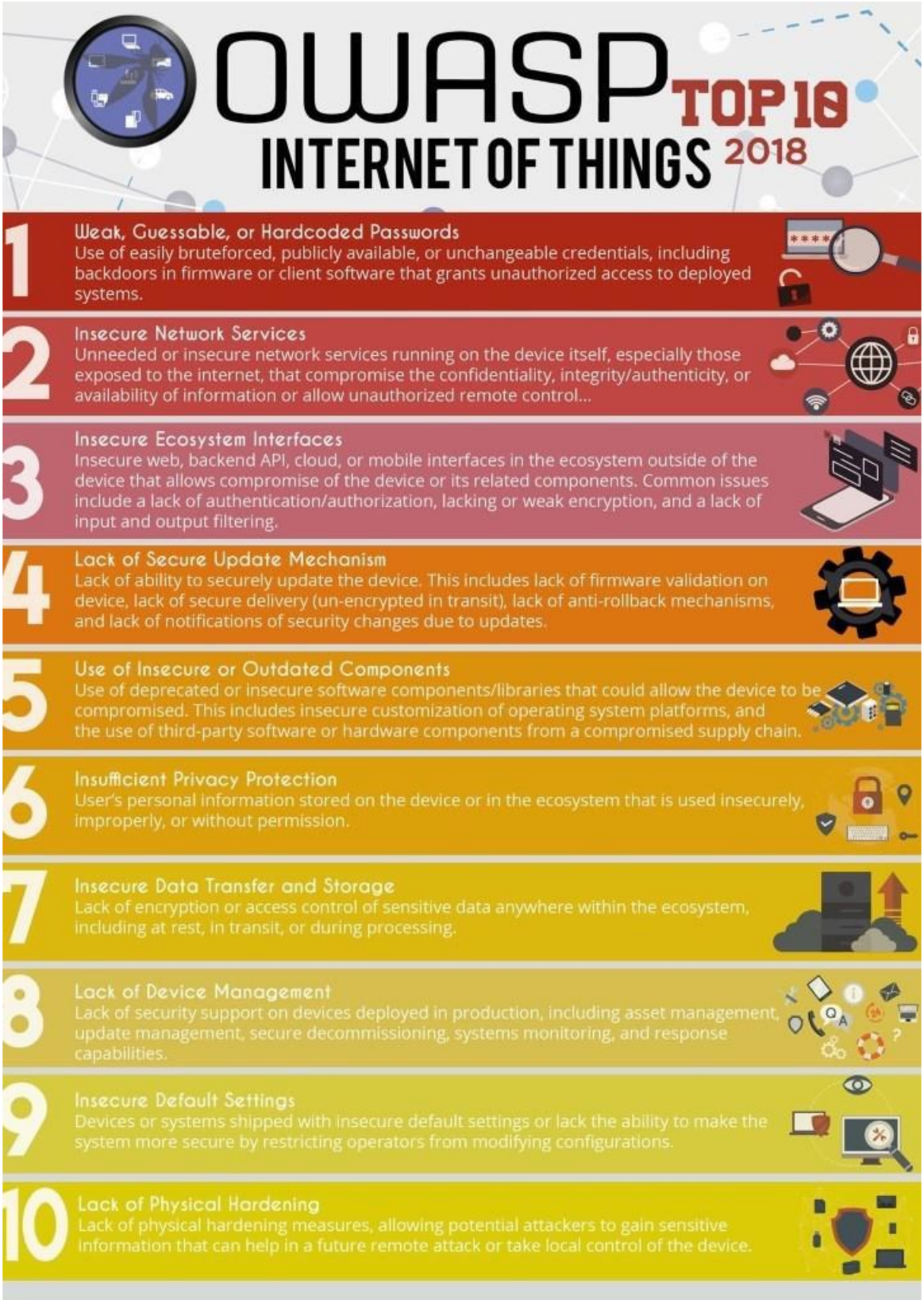

Figura 17- Figura 4 - OWASP Top 10 vulnerabilidades [66]

Conforme ilustrado na figura 4, os dispositivos IoT apresentam um alto potencial de riscos, e há pontos críticos que precisam de avaliação e compreensão aprofundadas. A lista dos "Top 10" da OWASP para IoT inclui os seguintes vetores de ameaça:

1. **Passwords fracas, de fáceis de adivinhar ou codificadas:**

Passwords vulneráveis que podem ser exploradas por ataques de força bruta, com listas publicamente disponíveis amplamente utilizadas em diversos dispositivos.

2. **Serviços de rede inseguros:**

Execução de serviços de rede desnecessários ou inseguros nos dispositivos IoT, especialmente aqueles expostos à internet, comprometendo a segurança das informações, autenticidade e disponibilidade, bem como permitindo controlo não autorizado remoto.

3. **Interfaces inseguras:**

Falhas comuns, como falta de autenticação, autorização insuficiente, criptografia fraca e ausência de filtragem de conteúdo nas entradas e saídas, que capacitam plataformas web inseguras, APIs na nuvem ou interfaces móveis fora do dispositivo, permitindo acesso não autorizado aos dispositivos ou seus componentes.

4. **Ausência de mecanismos de atualização:**

Incapacidade de atualizar dispositivos de maneira segura, incluindo validação inadequada do firmware, entrega não segura de atualizações, ausência de mecanismos anti-rollback e falta de notificações sobre alterações de segurança devido a atualizações.

5. **Utilização de componentes inseguros ou desatualizados:**

Uso de componentes e bibliotecas de software desatualizados ou inseguros, que podem comprometer a segurança do dispositivo, juntamente com a personalização inadequada do sistema operativo e o uso de hardware de terceiros.

6. **Proteção de privacidade insuficiente:**

Informações pessoais de utilizadores armazenadas no dispositivo ou no ecossistema que são usadas de maneira insegura, imprópria ou sem permissão.

7. **Transferência e armazenamento de dados inseguros:**

Falta de criptografia ou controlo de acesso inadequado para dados confidenciais em toda a rede, incluindo durante a transmissão, armazenamento ou processamento de dados.

8. **Falta de gestão de equipamentos:**

Ausência de suporte de segurança para dispositivos em produção, incluindo gestão de ativos, atualizações, desativação segura e monitorização de sistemas.

9. **Configurações padrão inseguras:**

Fornecimento de dispositivos ou sistemas com configurações padrões inseguras, que não permitem modificações para tornar o sistema mais seguro.

10. **Falta de bloqueios físicos:**

Ausência de medidas de proteção física, permitindo que invasores obtenham informações confidenciais para uso em ataques remotos futuros ou controlo não autorizado do dispositivo local.

Após uma análise minuciosa da lista "Top 10" de riscos fornecida pela OWASP, fica evidente que a gestão de riscos desempenha um papel crucial para empresas e organizações entenderem o que está em risco e como mitigar esses riscos. A implementação de ações adequadas é fundamental para gerir eficazmente o nível de risco.

A Lei 46/2018 de 13 de agosto [67] exige a adoção de medidas que garantam a resiliência e a mitigação de riscos de ataques, juntamente com a capacidade de responder eficazmente para restaurar os níveis de serviço num espaço de tempo definido e aceitável.

É importante destacar que os dispositivos IoT recolhem, transmitem e processam uma grande quantidade de dados. É crucial garantir que a transmissão de dados seja criptografada ou use mecanismos de autenticação eficazes. Esta recolha massiva de dados permite uma fácil monitorização das atividades de cada equipamento, utilizando sistemas cada vez mais sofisticados, existindo alguns dotados de capacidades de adaptação e de aprendizagem.

Os dados podem ser recolhidos automaticamente usando scripts, tornando essa tarefa simples e automatizada. Posteriormente, esses dados podem ser armazenados em base de dados para fácil acesso e consulta.

Com o acesso indiscriminado à internet, os dados são utilizados em vários sites e nos próprios equipamentos, sendo que o utilizador na maioria dos casos não tem uma noção clara do uso que é dado aos seus dados.

Para garantir a confidencialidade, é essencial utilizar mecanismos de criptografia robustos e modernos, mantendo a chave de criptografia em segredo. No entanto, a gestão dessas chaves é uma tarefa complexa, pois a exposição prolongada da chave representa um risco, uma vez que não existe uma rotatividade constante ou uma alteração frequente destas.

Os equipamentos que não estejam dotados de um sistema de confiança são um potencial risco. A troca de credenciais entre um serviço ou uma aplicação devem ser acauteladas e o relacionamento entre estas aplicações não deverá levantar suspeitas.

O controlo de acessos em equipamentos IoT é também um grande desafio por parte dos fabricantes dado existir uma grande abertura por parte destes para que qualquer equipamento se interligue, no entanto não existem medidas que tratem os direitos dos acessos concedidos a outros aparelhos IoT. Este risco deverá estar presente nas equipas de TI locais uma vez que a grande maioria dos equipamentos IoT tem pouco ou nenhum armazenamento interno, sendo difícil fazer uma análise posterior aos logs gerados por si.

A comunicação entre dispositivos IoT por meio de middleware também é um ponto de risco a ser considerado. Muitas vezes, os dados transferidos não possuem proteção adequada, o que dificulta o avanço da segurança e privacidade da tecnologia.

As redes programáveis estão em crescimento exponencial, mas é fundamental evitar a instalação de programas ou scripts que possam ter intenções maliciosas. Botnets são um exemplo de ameaça, onde robots conectados à internet realizam tarefas repetitivas, muitas vezes comprometendo dispositivos que tiveram sua segurança violada.

Desligar dispositivos da rede nem sempre é suficiente para garantir a segurança, pois muitos dispositivos IoT têm a capacidade de armazenar dados e transmiti-los quando reconectados à rede.

Atualmente, os dispositivos IoT geram uma quantidade massiva de informações, e a análise desses dados para extrair informações significativas representa um desafio devido à quantidade de informações geradas.

O malware é um tipo de ameaça que poderá alterar dados de um dispositivo e comprometer o diagnóstico, sendo destinado a realizar ações não autorizadas, podendo causar danos no equipamento ou na rede

Com a expansão do número de objetos, dispositivos e equipamentos, cada um com suas próprias interfaces, serviços e capacidades, a interoperabilidade emerge como um elemento fundamental para a integração perfeita de todos eles.

Uma rede interoperável possibilita a utilização de padrões técnicos partilhados, permitindo uma troca de dados e informações sem complicações. Portanto, para garantir que todos os dispositivos conectados comuniquem de maneira padronizada, minimizando riscos, é crucial que os desenvolvedores adotem uma linguagem que promova a harmonia entre os diversos sistemas interligados.

Quando se trata de protocolos de comunicação, o protocolo HL7 é amplamente reconhecido na área da saúde. Embora o HL7 já tenha uma ampla adoção global, ainda não é uma prática comum que todos os dispositivos que compartilham dados de saúde utilizem esse protocolo para o envio e recebimento de mensagens.

Os dispositivos da Internet das Coisas (IoT) estão particularmente vulneráveis a ataques, pois transmitem dados sem fio em intervalos definidos, o que facilita a execução de ataques de falsificação. Além disso, a transmissão e o processamento de dados enfrentam todas as questões de segurança já conhecidas que existem na rede TCP/IP.

As equipas de TI nas unidades de saúde devem estar cientes dos diversos pontos de entrada na rede e das vulnerabilidades presentes nos dispositivos IoT, que podem ser afetados por problemas de segurança no software, hardware e firmware.

3.7. Vulnerabilidades do IoT

A rápida expansão dos dispositivos IoT e a carência de medidas de segurança sólidas nestes dispositivos representam uma crescente ameaça à segurança e privacidade de indivíduos e empresas que os utilizam. Os dispositivos IoT consistem numa crescente variedade de componentes de software e hardware, resultando em complexidade significativa que dificulta a implementação de controlos de segurança abrangentes. Portanto, é crucial abordar a segurança de forma abrangente, considerando a interconexão de todos os elementos.

De acordo com a IETF-Internet Engineering Task Force no RFC 2828 [68] , uma "vulnerabilidade" é definida como uma fraqueza ou falha no design, implementação ou operação de um sistema que pode ser explorada para violar a política de segurança do sistema.

O projeto OWASP [69] lista as 10 principais vulnerabilidades do IoT que devem ser consideradas como base para avaliação em organizações ao desenvolverem ou implementarem projetos de IoT, são elas:

- Segurança física dos objetos/equipamentos inteligentes;
- Software/firmware vulnerável;
- Falta de criptografia e verificação de integridade dos dados;
- Configuração insuficiente na segurança dos objetos;
- Autenticação/autorização insuficiente nos equipamentos;
- Serviços de redes vulneráveis (privadas ou Internet);
- Interface da cloud vulnerável;
- Interface de gestão dos IoT vulneráveis;
- Interface móvel dos IoT vulneráveis;
- Privacidade de dados dos utilizadores de IoT.

É importante notar que a mera existência ou identificação de uma vulnerabilidade não representa uma ameaça imediata por si só. Para que um dispositivo seja comprometido, é necessário que exista uma ameaça que explore essa vulnerabilidade.

As unidades de saúde devem estar vigilantes e conscientes das ameaças aos vários pontos de entrada nas suas redes. Com centenas de dispositivos interconectados, cada um deles apresentando vulnerabilidades no seu hardware e software, é fundamental monitorizar de perto a segurança.

Os protocolos que possibilitam o acesso remoto são frequentemente os primeiros alvos de testes na procura de vulnerabilidades. Estas falhas são alvos frequentes de hackers e cibercriminosos, uma vez que muitas vezes são mal configuradas, com passwords fracas ou passwords padrão amplamente conhecidas e disponíveis na internet. O botnet Mirai [70] é um exemplo de como esses ataques são comuns.

Testes de penetração, ou pentest, são realizados para identificar e validar vulnerabilidades em dispositivos, determinando o que um invasor poderia ganhar após um ciberataque bem-

sucedido [71] . Esse tipo de teste é valioso para identificar vulnerabilidades conhecidas e tomar medidas para mitigá-las.

A exploração de vulnerabilidades muitas vezes ocorre através da tentativa de violação do sistema de autenticação, frequentemente por meio de ataques de força bruta, visando obter acesso às credenciais do dispositivo para obter privilégios.

Muitos dispositivos não adotam boas práticas de segurança de rede, não exigindo passwords fortes ou complexas. Estes, frequentemente, são programados com passwords fracas ou previsíveis, e as passwords padrão são amplamente documentadas nos manuais disponíveis nos sites dos fabricantes. Exemplos comuns incluem passwords como "admin" ou "12345".

Existem várias ferramentas gratuitas que automatizam estes tipos de ataques de autenticação, incluindo tentativas de força bruta ou o uso de passwords padrão. Alguns exemplos dessas ferramentas incluem Hydra, Medusa ou NCrack, disponíveis na distribuição Kali Linux.

Outra vulnerabilidade significativa diz respeito à falta de atualizações regulares ou periódicas de segurança para muitos dispositivos IoT, que frequentemente permanecem com configurações padrão consideradas inseguras.

A transferência e armazenamento de dados muitas vezes não são criptografados, o que torna relativamente fácil intercetar os dados transmitidos. Além disso, dispositivos menores podem ser roubados, permitindo a análise dos dados fora do contexto em que são gerados.

A maioria dos fabricantes de dispositivos IoT deixa portas de acesso abertas (backdoors) para oferecer suporte, caso necessário. Isso é feito para entender melhor o comportamento dos consumidores e melhorar as funcionalidades dos dispositivos, mas gera uma grande quantidade de informações (BIG DATA) que precisa ser tratada. É essencial entender que tipo de telemetria está a ser enviada pelos dispositivos e quais portas estão abertas, bloqueando o acesso a esses dispositivos e portas nas firewalls de perímetro.

Os dispositivos IoT são uma combinação de hardware e software que se comunicam por meio do firmware. O firmware original pode ser substituído por um firmware malicioso que altera o funcionamento do dispositivo. Analisar o firmware é uma maneira fundamental de identificar outras vulnerabilidades. O firmware está frequentemente disponível no site do fabricante, o que aumenta o risco de explorar seu código-fonte, mesmo sem acesso direto ao dispositivo.

A maioria dos dispositivos IoT possui uma aplicação web acessível pela internet para gestão, configuração ou monitorização. Estas páginas são alvo de ataques contantes, seja por SQL injection [72] , onde esta vulnerabilidade permite correr código SQL de forma não autorizada com o intuído de ler ou alterar dados de uma base de dados, de forma a executar código não autorizado. Outra vulnerabilidade conhecida para comprometer as plataformas web é o CROSS-Site Scripting (XSS). Esta vulnerabilidade consiste na execução de código malicioso através do browser quando é acedido. Este código pode ser utilizado com vários fins e proveitos sendo que a o principal objetivo foca-se na obtenção dos cookies de autenticação para escalar privilégios.

A adoção lenta de padrões [73] é outro fator a ser considerado, uma vez que os dispositivos IoT frequentemente seguem padrões diferentes, tornando mais difícil a gestão, já que cada dispositivo tem seu próprio método de autenticação, armazenamento, comunicação e transferência de dados.

Em resumo, a maioria dos dispositivos IoT tem recursos limitados, com microcontroladores de baixo custo e memória limitada. Estas características tornam a migração para controladores de IoT desafiadora, pois os protocolos de internet existentes geralmente não são projetados para dispositivos com essas funcionalidades adicionais. A classificação de vulnerabilidades é fundamental para atribuir um valor ao nível de risco, normalmente usando uma escala de 0 a 10 [74] , embora essa classificação possa ser subjetiva dependendo da interpretação dos resultados obtidos. Existem padrões estabelecidos para classificar o risco de vulnerabilidades, ajudando a avaliar a gravidade das ameaças.

3.8. Síntese

Neste capítulo, conduzimos uma revisão abrangente do conhecimento científico na área dos dispositivos IoT, que é relevante para o contexto deste trabalho. O objetivo principal foi apresentar de forma abrangente os conceitos essenciais para compreender o funcionamento desta tecnologia.

Na primeira seção deste capítulo, além de oferecer um breve panorama histórico, encontramos, também, os diferentes tipos de comunicação empregados por esta tecnologia. São abordados os protocolos de comunicação mais comuns, com ênfase nos protocolos MQTT, CoAP e HTTP.

Como se trata de um trabalho direcionado para lidar com informações clínicas ou de saúde, também são apresentadas as normas de comunicação standards mais enraizadas neste setor, são elas o HL7, Dicom e OpenEHR.

Após esta análise mais científica tornou-se imprescindível analisar quais os tipos de ataques e os tipos de ameaça a que estes tipos de equipamentos IoT estão propensos, analisando também os variados riscos e vulnerabilidades.

4. Caracterização de equipamentos IoT

Os dispositivos IoT nas instalações de saúde representam uma crescente tendência, conectando-se à rede, estabelecendo interconexões e gerando continuamente informações. Estes dispositivos são reconhecidos como objetos inteligentes, robustos, capazes de criar as suas próprias redes independentes com infraestruturas e protocolos dedicados.

Neste capítulo, exploramos uma variedade de dispositivos IoT encontrados em ambientes de saúde, examinando os tipos de ataques comuns que cada dispositivo enfrenta. Estes dispositivos podem operar ativamente na rede, transmitindo e recebendo informações, ou podem funcionar passivamente, armazenando dados em sensores para posterior leitura. Uma das suas principais características é a capacidade de fornecer dados de forma precisa e instantânea, preenchendo a lacuna entre o mundo digital e o mundo físico, eliminando erros de transcrição humanos.

A utilização desses dispositivos em instalações de saúde visa recolher informações de maneira precisa e sem intervenção humana, reduzindo a possibilidade de erros na leitura ou recolha de dados. Estes dispositivos podem recolher dados de forma confiável em horários específicos e com consistência ao longo do dia, permitindo que os profissionais de saúde se concentrem em outras tarefas relacionadas ao atendimento médico.

É importante notar que estes dispositivos geralmente estão conectados à rede da instituição de saúde, e nem todos são dispositivos médicos. Alguns equipamentos que são considerados problemáticos como é o caso de uma impressora, por exemplo, equipamento presente em qualquer modelo de negócio, no entanto pode ser o foco de entrada para um ataque como irá ser abordado e ganha o título de IoT a partir do momento que é ligado à rede.

A seguir, listamos alguns exemplos de dispositivos que podem estar conectados à rede numa instalação de saúde:

4.1. Equipamentos clínicos

Em unidades de saúde, a panóplia de equipamentos ligada á rede é muito diversificada, no entanto, no âmbito deste projeto foram identificados os principais equipamentos clínicos que se encontravam ligados na rede no momento.

Após identificar esses dispositivos clínicos, examinamos os riscos e vulnerabilidades mais comuns associados a cada um deles, com base na revisão do estado da arte previamente realizada.

4.1.1. Dispensadores de Medicação

Figura 18-Dispensador de medicamentos automático

Os dispensadores de medicação são utilizados nas unidades de saúde com farmácia hospitalar integrada. São equipamentos que na sua maioria detêm um sistema operativo descontinuado e/ou obsoleto, que integram diversos equipamentos mecânicos, entre eles gavetas que na sua maioria foram concebidos para funcionarem com um determinado sistema operativo, como é o caso do Windows XP que deixou de ser suportado em fevereiro de 2015, e o Windows 7 deixará de ter suporte em janeiro de 2020. Apesar de funcionarem corretamente e cumprirem

com a função para o qual foram concebidos, não existe uma sensibilização por parte dos administradores para procederem a um novo investimento para aquisição de equipamentos mais recentes.

Existem por exemplo equipamentos com Windows XP com controladores de hardware que também deixaram de ter suporte com outras versões de Windows mais atuais, inviabilizando assim o uso do equipamento, independentemente de atualização do sistema operativo. É perentório que os fabricantes trabalhem lado a lado para possibilitarem a continuidade de negócio, acompanhado a evolução de todo o ecossistema.

Estes equipamentos, são autênticos robots que possibilitam a triagem, a separação e a rotulagem de medicação corretamente, para dispensa à cabeceira do utente.

São equipamentos que estão suscetíveis a ataques de ransomware, e por consequência à negação de serviço, ou à manipulação da informação, podendo causar efeitos negativos no tratamento do doente.

Caso o equipamento fique inoperacional, a garantia da distribuição da medicação atempadamente fica comprometida, sendo necessário reforçar as equipas para fazer a distribuição dos fármacos e a respetiva etiquetagem.

Se o equipamento for atacado e se o cibercriminoso proceder à alteração da medicação por cama este poderá comprometer a segurança do utente.

Os dados recolhidos podem também ser capturados e vendidos no mercado negro, expondo assim o tratamento que cada utente teve direito, identificado por exemplo se um dado utente tem algum distúrbio psíquico em função do fármaco que lhe foi administrado, ou alguma doença grave que inviabilize um crédito ou um seguro de vida.

São equipamentos que ajudam muito os profissionais de saúde nas suas tarefas diárias, pelo que deverão ser tomadas medidas de segurança para garantir que o equipamento não fique exposto na rede a ataques conhecidos.

4.1.2. Estações de Aquisição de Imagem

Figura 19-Estação de Aquisição de imagem

As estações de aquisição de imagem são utilizadas para diagnosticar um elevado leque de doenças, e permitem visualizar em tempo real diversas partes internas do organismo, capturando imagens para posterior análise e relatório.

Na sua maioria, todos estes equipamentos integram com um PACS (Sistema de Comunicação e Arquivo de Imagens) e estão interligados por rede utilizando o protocolo TCP/IP para comunicar entre si enviando as imagens com o protocolo DICOM.

Estes equipamentos estão suscetíveis a ataques de negação de serviço, ou a ataques de man-in-the-middle, sendo possível intercetar as imagens capturadas, e arquivá-las por exemplo em nome de outro utente, ou simplesmente descartá-las. Este tipo de ação pode levar a diagnósticos errados por parte das equipas médicas, causando efeitos nefastos ao utente sem que ninguém se aperceba do que ocorreu. É uma prática de terrorismo clínico que pode ser utilizada para causar ausência de cuidados, ou cuidados errados.

São equipamentos muito caros, sujeitos a concursos públicos de aquisição, onde são efetuados contratos de manutenção para garantir a disponibilidade do equipamento. No entanto os updates de firmware nem sempre são contemplados, pelo que se deverá ter especial atenção ao que é contratualizado.

4.1.3. Monitores de Sinais Vitais

Figura 20-Monitor de sinais vitais

Os monitores de sinais vitais tal como o nome indicam, monitorizam os sinais vitais de um utente, nomeadamente os batimentos cardíacos, a tensão arterial, a temperatura, e a oxigenação. Existem monitores que fazem também um ECG (eletrocardiograma), um exame de rotina que avalia o ritmo dos batimentos cardíacos.

Estes monitores emitem alertas para auxiliar as equipas de cuidados médicos, para uma rápida atuação em caso de ausência de sinais vitais.

A principal vulnerabilidade deste equipamento foca-se na ausência de autenticação do protocolo que utiliza na comunicação, podendo ser possível emular informações falsas às equipas médicas, disponibilizando valores diferentes dos reais comprometendo a saúde e o bem-estar do paciente.

É fulcral analisar se os dados transmitidos por este tipo de equipamentos, é encriptado. Existem relatos [75] de equipamentos que transmitem os dados em cleartex[3]. Os dados extraídos destes equipamentos podem assim ser capturados e colocados á venda em mercados negros, apresentando um historial clínico de um determinado utente, inviabilizando a estes por exemplo o acesso a seguros de saúde ou a créditos na banca, caso estas empresas tenham conhecimento prévio dos futuros clientes.

[3] Termo utilizado em informática que define que não existe encriptação ou que é possível ler o que é transmitido.

4.1.4. Bombas de Perfusão

Figura 21-Bomba de perfusão

As bombas de perfusão, permitem injetar líquidos no corpo humano, nomeadamente fármacos ou nutrientes, com um preciso controlo de fluxo e de volume nas vias venosas ou arteriais.

Este tipo de equipamento auxilia as equipas médicas ao administrar quantidades certas e precisos e com ciclos pré-definidos de medicação, evitando a deslocação de um médico ou de um enfermeiro constantemente junto do doente para esta tarefa. Apesar das suas vantagens estes equipamentos têm algumas interfaces de comunicação, nomeadamente, portas USB e portas de rede para configuração e monitorização nos mais variados cenários.

O acesso á bomba também pode ser feito por um portal web, com passwords fracas ou por defeito, onde pode ser definido os fluxos e as quantidades que são injetadas. A comunicação não é criptografada pelo que poderá ser possível capturar o tráfego.

São equipamentos que não costumam receber updates de firmware automáticos, pelo que poderão ter as suas fragilidades já conhecidas a descoberto.

O acesso indevido por pessoas mal-intencionadas a este tipo de equipamentos pode ser utilizado para causar prejuízo na vida do utente, ou para recolha de informação e posterior comércio da informação em mercados negros.

4.1.5. Bombas de Insulina

Figura 22-Bomba de insulina

As bombas de insulina são utilizadas diariamente por diabéticos que entregam o seu bem-estar a estes equipamentos ficando assim despreocupados com a dosagem de insulina que lhes é administrada sendo esta responsabilidade incutida ao equipamento.

São equipamentos que já contam com vulnerabilidades conhecidas [76] , nomeadamente ao nível da comunicação sem fios uma vez que não dispõem de autenticação nem autorização.

Assim devem ser tomadas medidas para evitar que estes equipamentos coloquem em risco vidas humanas, seguindo as indicações do fabricante, atualizando para os firmware mais atuais quando estes são disponibilizados.

Estes equipamentos são transportados pelos utentes, para dentro e para fora das unidades de saúde, pelo que se tornam um potencial risco, uma vez que pode existir utentes com ideias de violar a segurança da informação, e injetar neste tipo de equipamentos vírus ou malware que poderá ter impacto na rede da unidade de saúde.

4.1.6. Vídeo-Cápsula

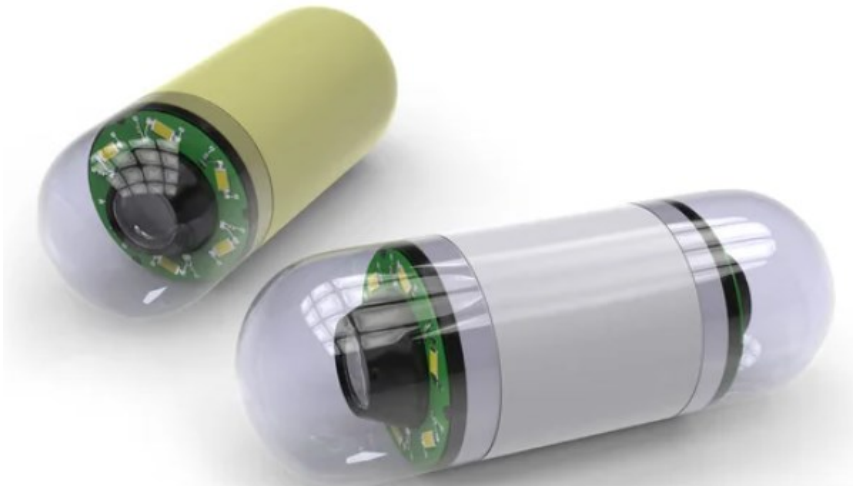

Figura 23-Vídeo-Cápsula

A vídeo-cápsula utilizada para diagnosticar problemas do trato digestivo, examina cada detalhe percorrendo todo o trajeto dos alimentos em todo o seu percurso digestivo.

A cápsula está dotada de uma camara fotográfica e de um flash, e vai capturando fotos a cada instante. O utente por norma traz um recetor à cintura onde as imagens vão ser recolhidas.

Estas cápsulas por norma não trazem métodos de autenticação, sendo possível intercetar as imagens enviadas para o recetor. Apesar de não causar grande impacto, este tipo de ataques pode levar á repetição do exame causando prejuízo no utente ao não ter a doença diagnosticada atempadamente.

4.1.7. Esfigmomanómetros

Figura 24-Esfigmomanómetro

Os esfigmomanómetros são aparelhos utilizados na sua génese para verificar a tensão arterial e a pulsação arterial do utente. São equipamentos de uso pontual, pelo que não são utilizados para fazer uma monitorização continua. Alguns equipamentos deste tipo permitem a ligação á rede para descarregar as leituras efetuadas.

São equipamentos que podem sofrer de ataque man-in-the-middle, pelo que os dados anexados a um processo clínico podem não ser os dados realmente obtidos, levando as equipas médicas a um diagnóstico errado. A não atualização deste tipo de equipamentos também pode comprometer outros equipamentos de rede, podendo este ser utilizado para explorar falhas ou vulnerabilidades presentes na infraestrutura da unidade de saúde.

São equipamentos que têm portas rs232 ou portas usb disponíveis que não são utilizadas, pelo que a presença deste tipo de ligações pode ser explorada para obter outro tipo de privilégios.

4.1.8. Pacemaker

Figura 25-Pacemaker

O pacemaker é um dispositivo médico que tem como objetivo regular os batimentos cardíacos de um doente.

São equipamentos que possibilitam acesso por intermédio de um aparelho intermédio denominado MICS (Medical Implant Communication Service). Este MICS é ligado ao computador onde possibilita fazer um check-up ao pacemaker, assim como configurar a cadência ou o ritmo a incutir no coração.

São equipamentos que necessitam de uma intervenção cuidada e cautelosa para implementação, uma vez que é necessária uma cirurgia evasiva. É um equipamento fulcral á vida humana e que pode levar á morte se for mal configurado.

Um pacemaker ao ficar comprometido ao nível de segurança tem como principal risco levar o paciente á morte, ou sob o risco de o paciente ter que ser sujeito a nova cirurgia para remover o equipamento em questão.

4.1.9. Monitor de Glicose

Figura 26-Monitor de Glicose

Os diabéticos, necessitam controlar os níveis de glicose regularmente para não sofrerem nenhuma hipoglicémia ou hiperglicemia. Estas duas patologias podem ser fatais se os valores de glicémia forem substancialmente baixos, ou substancialmente altos respetivamente.

Assim, com os monitores de glicose, os diabéticos conseguem equilibrar os níveis de glicose, podendo administrar mais ou menos insulina, em função dos valores apresentados.

Existem equipamentos que carecem de uma lanceta que perfura o dedo para obter uma gotícula de sangue para análise.

Estes equipamentos recolhem os dados que posteriormente podem ser analisados por um profissional de saúde em gráfico ou em tabelas no computador.

Existem também equipamentos (por exemplo o FreeStyle Libre) que prescindem da lanceta, sendo apenas necessário encostar o equipamento ao braço para efetuar a leitura.

O principal risco da utilização deste equipamento está relacionado com a alteração de valores, e de uma possível sobredosagem na dose de insulina a administrar. Ao ligar estes equipamentos à rede é fundamental que os computadores locais tenham políticas de segurança bem definidas e as últimas atualizações dos antivírus instaladas de forma a mitigar uma possível intrusão, ou contaminação de malware que poderá ter efeitos em toda a infraestrutura.

4.2. Equipamentos de suporte e periféricos

Uma unidade de saúde tem presente na sua infraestrutura de rede variadíssimos equipamentos de suporte e outros periféricos que possibilitam funcionalidades de logística, de monitorização ou de alarmística, que não são exclusivos de uso clínico.

Este tipo de equipamentos ajuda a monitorizar outros sensores para garantir o bom funcionamento do modelo de negócio das unidades de saúde. São equipamentos que não lidam diretamente com dados clínicos, no entanto são fundamentais para a continuidade do negócio.

São equipamentos que ganham o estatuto de IoT a partir do momento que são ligados à rede, partilhando informações que podem ser extraídas e analisadas. São também equipamentos que são utilizados no dia-a-dia como é o caso das impressoras e frigoríficos. Equipamentos banais que na sua génese foram comprados com o propósito a que se destinam, mas que possibilitam outro tipo de funcionalidades, colocando em risco a instituição de saúde.

4.2.1. Pulseiras de identificação de bebês

Figura 27-Pulseira anti rapto

O despacho n.º 20730/2008 do decreto de lei nº 152 de 7 de agosto de 2008 veio obrigar as unidades de saúde a utilizarem pulseiras nos recém-nascidos de forma a evitar o rapto e a troca de crianças.

Estas tags ou pulseiras garantem que um determinado bebé corresponde a uma determinada mãe sendo possível localizar o bebé dentro do edifício com recurso á triangulação do sinal da rede wi-fi.

Caso a tag se aproxime de uma zona de saída não autorizada o sistema gera um alarme automático com a indicação do bebé que se aproximou dessa zona, acionando medidas preventivas, nomeadamente o fecho de portas, bloqueio de elevadores, sinalização luminosa e acústica.

Se o sistema for violado, será possível iludir o sistema criando a ilusão que o bebé se encontra em determinada zona, quando na realidade poderá já estar fora do edifício.

De salientar que os routers utilizados poderão ter as credenciais de acesso por defeito ou nunca terem sofrido atualizações de firmware.

4.2.2. Sensores de temperatura

Figura 28-Sensor de temperatura

Os sensores de temperatura, recolhem com alta precisão os valores de temperatura, humidade e ou a pressão atmosférica de um dado local. Nas unidades de saúde são muito utilizados para garantir a temperatura correta no acondicionamento da medicação.

A alteração forçada destes valores pode levar ao prejuízo em milhares de euros em medicação, ou poderá ter efeitos negativos se o sensor indicar uma temperatura falsa, mas na realidade estiver a debitar outra.

Estes sensores geralmente funcionam em paralelo com os sistemas de arrefecimento (chiler ou ar condicionado), pelo que a atmosfera será refrigerada ou aquecida em função da leitura que for efetuada pelo sensor de temperatura.

4.2.3. Sensores de dióxido de carbono

Figura 29-Sensor de Dióxido de Carbono

Os sensores de dióxido de carbono permitem monitorizar um determinado lugar, analisando a qualidade do ar permanentemente, verificando se existe a presença de dióxido de carbono (CO2).

Estes equipamentos permitem a ligação á rede, onde é possível configurar parâmetros e extrair dados para estatística.

Existe ainda a possibilidade de configurar os equipamentos para acionar uma ação após um determinado valor. A título de exemplo, é possível abrir janelas automáticas e ligar os extratores de ar quando se verificar um determinado valor elevado de CO2.

O maior risco associado a este equipamento poderá estar na captura dos dados, e informar posteriormente os variados sensores de valor errados, falsificando a leitura correta.

É fundamental atualizar o equipamento com os últimos updates de firmware e proceder à alteração das passwords por defeito para passwords com maior grau de complexidade e diferentes de outros equipamentos. Uma pessoa mal-intencionada pode tentar o controlo indevido sobre um equipamento mais pequeno, sem tanto impacto e explorar a utilização dessa password em outro equipamento da rede.

4.2.4. Portas automáticas

Figura 30-Porta Automática

As portas automáticas, tem um dispositivo de comunicação que permite o seu controlo através de um servidor web ligado á rede por TCP, onde é percetível o histórico de incidências (aberturas/fechos), trincos, e inclusive é possível controlar o horário de funcionamento da porta.

Atualmente a facilidade com que se abre e fecha uma porta de forma remota poderá trazer riscos para a segurança do edifício, uma vez que os servidores que controlam as portas podem ser atacados por pessoas mal-intencionadas, proporcionando o roubo de bens ou vedando o acesso a pessoas ao edifício.

É fulcral atribuir estes acessos apenas a funcionários credenciados para o efeito, sensibilizando-os para os ataques de engenharia social que poderão ser levados a cabo para ter acesso á instituição.

4.2.5. UPS (Fontes de alimentação ininterruptas)

Figura 31-UPS

As UPS ou as fontes de corrente estabilizada, garantem que um aparelho não fica com ausência de corrente elétrica, assegurando que a corrente que lhe chega é estabilizada e isenta de tensões anormais.

Estes equipamentos permitem a ligação a um web server onde é possível verificar que energia está a ser debitada em cada saída, verificar os logs de interrupção de serviço, e em alguns equipamentos é possível fazer um reboot remoto.

Este tipo de equipamento ganha o estatuto de IoT a partir do momento que é ligado á rede, para ser monitorizado. É com esta ligação de rede que passa a ser um equipamento vulnerável, dado não possuir autenticação cifrada é possível a pessoas mal-intencionadas desligarem equipamentos de cariz fulcral na instituição indevidamente ou propositadamente.

4.2.6. Impressoras

Figura 32-Impressora

Apesar da desmaterialização do papel que se tem vindo a fazer sentir, as impressoras ainda são um equipamento presente e fundamental nas unidades de saúde. O principal risco destes equipamentos quando ligados á rede por TCP/IP foca-se na disponibilização do webservice, onde poderá ser possível capturar os documentos da fila de trabalho e ter assim acesso a documentos de cariz confidencial.

Cada vez mais se imprime menos, no entanto o risco de encontrar uma impressora vulnerável com um firmware desatualizado é grande, pelo que poderá ser utilizado por pessoas mal-intencionadas para adquirir informação preciosa para ajudar num ataque de engenharia social.

As impressoras também podem ser utilizadas para aceder a outros equipamentos da rede, ou seja, podem facilmente tornar-se a "máquina de salto" para ajudar a entrar na rede, isto é, algumas impressoras têm a ligação Wi-fi aberta, que por sua vez têm uma ligação direta ou indireta a um computador. Assim torna-se perentório que as unidades de saúde olhem para as impressoras como um equipamento a ter em conta ao nível da cibersegurança.

Em agosto de 2018, a HP. corrigiu centenas de modelos a jato de tinta vulneráveis a duas falhas de execução remota de código disponibilizando as respetivas falhas na lista de vulnerabilidades comuns (CVE-2018-5924, CVE-2018-5925).

Um estudo patrocinado pela HP[77] constatou também que 56% dos entrevistados, alegam não ter qualquer tipo de política de segurança para as impressoras ligadas à rede nas organizações.

4.2.7. Controladores de Autómatos

Figura 33-Controlador de Gerador

Os demais variadíssimos autómatos utilizados para controlar por exemplo bombas de água, elevadores, geradores, quadros elétricos, entre outros, são equipamentos que se encontram ligados á rede na sua maioria por via de um computador.

Os mais vulneráveis, são na sua génese equipamentos com alguma idade, colocados em produção aquando da inauguração dos edifícios e cuja sua modernização estagnou, no entanto desempenham a função para o qual foram programados, não havendo necessidade de efetuar atualizações sob risco de este se tornar inoperacional.

Apesar da sensibilização das equipas de tecnologias de informação, estes autómatos ainda se encontram nas redes e são um foco que deve ser sanado.

Os autómatos mais recentes já permitem a atualização de firmware e não estão dependentes de um computador com aplicações proprietárias para servir de interface na ligação.

Os principais riscos focam-se na negação de serviço, e no impacto que podem causar no negócio.

4.2.8. Controlos de Acesso

Figura 34-Controlador de acesso

Os controlos de acesso permitem abrir e fechar portas, assim como permitem fazer a gestão de pessoal, permitindo efetuar o controlo das horas a que iniciaram e terminaram a sua produção.

São sistemas que apesar de funcionarem com a impressão digital, têm sempre um método alternativo para não se tornarem inoperacionais. A título de exemplo existem profissionais com a impressão digital muito ténue que não conseguem fazer a sua leitura nestes equipamentos. Existe também a possibilidade de uma pessoa ter um acidente e ficar com os dedos registados na base de dados inoperacionais. Assim, para colmatar estas falhas ou contornar estas dificuldades os fabricantes permitem registar utilizadores com acesso a um pin ou um código, evitando assim a inviabilização do equipamento.

Estes equipamentos por norma geral também tem um utilizador por defeito para possibilitarem em caso de necessidade o acesso a forças de segurança (exemplo: bombeiros e polícia) evitando que danifiquem a porta em questão.

O acesso por pessoas mal-intencionadas a este equipamento, comprometendo a integridade, permite a indisponibilidade de serviço, que se poderá traduzir numa ação catastrófica quando se pretende controlar o acesso a uma unidade de saúde. Estes tipos de instituições têm por vezes mais de mil funcionários que poderão ficar impossibilitados de entrar no edifício.

A captura dos dados destes funcionários também pode ser usada para realizar ataques de engenharia social, uma vez que é possível perceber as rotinas dos funcionários e os fluxos de acesso.

4.2.9. Quiosques de pagamento automático

Figura 35-Quisosque de Pagamento Automático

Os quiosques de pagamento são utilizados para tornar os edifícios mais práticos e fluidos, reduzem o tempo de espera aos utentes uma vez que possibilitam ao utente efetuar pagamentos e admissões autonomamente sem necessidade de intervenção de um funcionário da instituição.

Estes equipamentos são equipados com dispensadores de passwords e um cofre mealheiro, ou um terminal de multibanco, onde é possível efetuar pagamentos, a admissão a uma determinada consulta e pagar as taxas moderadoras em dívida.

Estes quiosques, na realidade são vulgares computadores que dispõem de diversos periféricos instalados para funcionarem de forma muito simples e intuitiva por intermédio de um touchscreen. Ao tratar-se de computadores, são equipamentos ligados á rede e suscetíveis a ataques.

A negação de serviço e o pagamento indevido de taxas moderadoras são exemplos de ataques que podem ocorrer nestes equipamentos. É perentório que estejam atualizados, no entanto, dado tratar-se de um conjunto de periféricos, nem sempre é fácil garantir o funcionamento dos diversos periféricos instalados com as diferentes atualizações de sistema.

4.2.10. Central telefónica

Figura 36-Central Telefónica

A central telefónica de uma unidade de saúde é um equipamento muito importante e fundamental para a continuidade do negócio de uma unidade de saúde. Existem centrais telefónicas analógicas e digitais.

As centrais telefónicas têm um teclado que permite a interface entre o computador e o telefone, sendo possível reencaminhar chamadas, gravar, colocar em espera, entre outras funcionalidades que as consolas permitem de forma muito fácil e intuitiva para o utilizador.

Como principal ameaça, estes equipamentos de serviço estão suscetíveis à negação de serviço ou á captura de informação de acesso confidencial ou restrito, sendo fundamental as atualizações de firmware e do sistema operativo.

4.2.11. Câmaras de videovigilância ou webcams

Figura 37-Câmaras de videovigilância ou Webcams

As câmaras de videovigilância ou as webcams são equipamentos que possibilitam a vigilância de pessoas, bens ou de um determinado local em tempo real, podendo ser captado áudio e vídeo no presente momento. Alguns equipamentos estão dotados de motor, que são possíveis controlar remotamente, possibilitando assim alargar o espectro de visão da câmara, alcançando outros locais com mais detalhe. São equipamentos que na sua maioria não sofrem updates de firmware automaticamente. Os fabricantes disponibilizam um portal web para configuração do equipamento com passwords por defeito, como por exemplo o tradicional admin de utilizador e admin de password.

O vídeo transmitido pode ser capturado por pessoas mal-intencionadas se não forem garantidos métodos de autenticação eficazes e uso de protocolos encriptados. Este vídeo ou as imagens capturadas, podem ser usadas para recolher informações confidenciais, perceber rotinas, explorando assim a vertente da engenharia social.

A negação de serviço, o DDoS ou a manipulação de informação são as principais falhas a que estes equipamentos estão propensos.

4.2.12. Sistema de Transporte Pneumático

Figura 38-Sistema de transporte Pneumático

Os sistemas de transporte pneumático, conhecidos como besidróglio são utilizados em unidades de saúde para enviar amostras de sangue, urina ou outras, diretamente para o laboratório de forma a evitar perca de tempo no transporte destes contentores.

São sistemas que funcionam a vácuo, onde os "torpedos" viajam numa rede de tubos espalhados por diversos locais sensíveis e que permite um transporte rápido e uma receção imediata deste tipo de cápsula.

Este sistema é controlado por um servidor que regista todos os eventos, nomeadamente que terminal envia e que terminal recebe um determinado torpedo, informando também de uma avaria caso esta ocorra, podendo especificar ao detalhe a tubagem onde ocorreu o congestionamento.

Este sistema sendo alvo de um ataque por uma pessoa mal-intencionada poderá causar negação de serviço pelo que afetará o habitual fluxo de trabalho colocando em risco o trabalho dos diversos funcionários, uma vez que a indisponibilidade deste equipamento poderá inviabilizar o envio das amostras para o laboratório, não havendo o resultado das análises atempadamente, ou poderá ter que haver necessidade de efetuar nova recolha de colheita ao utente uma vez que as amostras recolhidas podem ter sido desviadas para outro local.

4.2.13. Balanças

Figura 39-Balança de Laboratório

As balanças são usadas em unidades de saúde em diversos departamentos. Nas farmácias são utilizados para preparação de manipulados, nos laboratórios para medições de amostras clínicas, em contexto de consulta ou internamento para pesar o utente

Não é um equipamento fulcral aos cuidados de saúde nem coloca em risco a vida humana, no entanto é um equipamento que não deve ser descurado ao nível de segurança dado que possui um IP e se encontra ligado á rede, podendo uma pessoa mal-intencionada aproveitar-se das vulnerabilidades destes equipamentos para escalar privilégios na rede e conseguir acesso indevido a outros equipamentos.

4.2.14. Frigorifico

Figura 40-Frigorífico de Banco de Sangue

Os frigoríficos inteligentes, com ligação á rede, para monitorização constante de temperatura, encontram-se em algumas unidades de saúde, onde são guardados medicamentos que carecem de uma determinada temperatura especifica constante.

São equipamentos cuja segurança pode ser comprometida, colocando em risco outros equipamentos da rede. Pode ser utilizado como máquina de salto para chegar a outros equipamentos.

São equipamentos que em princípio não colocam em risco vidas humanas, no entanto deverão ser inventariados e identificados como potenciais portas de entrada para pessoas mal-intencionadas, uma vez que podem ser utilizados para escalar privilégios na rede em que estão ligados.

4.3. Síntese

Neste capítulo, foram delineados os principais dispositivos conectados a redes em unidades de saúde, destacando os riscos e vulnerabilidades associados à sua implantação numa análise prévia adequada. Os dispositivos analisados foram agrupados em duas categorias: equipamentos clínicos e equipamentos de suporte ou periféricos. Para cada dispositivo, enfatizamos o papel que desempenha na organização, sem negligenciar os riscos ou desafios que podem surgir quando estão na mesma rede.

Os dispositivos caracterizados são suscetíveis a falhas de disponibilidade ou a ameaças que podem comprometer a qualidade dos cuidados prestados aos pacientes. Portanto, é fundamental estar atento a ataques como ransomware, man-in-the-middle e negação de serviço (DDoS). Esses ataques podem ter sérias consequências para os pacientes, colocando em risco a sua capacidade de receber tratamentos adequados se os dispositivos de que dependem estiverem vulneráveis ou expostos a ameaças potenciais.

O próximo capítulo apresentará as principais diretrizes para a implementação de dispositivos IoT em unidades de saúde, destacando as principais fraquezas ou vulnerabilidades que podem resultar de uma implementação que ignore essas orientações.

5. Regras para implementação de IOT

Este capítulo tem como principal objetivo auxiliar as equipas de profissionais que fazem parte dos serviços de sistemas de informação de organizações de saúde, destacando regras de implementação e evidenciando boas práticas para a implementação de dispositivos IoT. O intuito é mitigar alguns dos riscos e vulnerabilidades mencionados no capítulo anterior.

Para que a implementação bem-sucedida e segura de IoT seja alcançada em unidades de saúde, é fundamental seguir boas práticas durante o processo de implementação. No entanto, dois aspetos são cruciais: controlo e confiança. As equipas locais devem manter o controlo sobre os dispositivos que estão a ser instalados e, ao mesmo tempo, transmitir confiança aos utilizadores das unidades de saúde em relação ao uso desses dispositivos. No entanto, essa sincronia nem sempre é fácil de alcançar na prática.

Para enfrentar esses desafios, atualmente existem diversos guias e frameworks que ajudam a estabelecer controlos em projetos de IoT, como o IoT Trust Framework [78] e o IoT Security Guidance [79] . Essas frameworks são usadas globalmente por algumas organizações para promover melhores práticas de segurança. Embora não sejam especificamente voltadas para unidades de saúde, os controlos apresentados nestes guias foram estudados e adaptados para se adequar ao contexto deste relatório.

Cada modelo de negócio possui características específicas, mas quando se trata de bens de valor monetário ou relacionados à saúde, a motivação para comprometer a segurança torna-se mais significativa, uma vez que isso afeta algo de valor para todos nós: a nossa saúde, bem-estar e futuro.

A indústria 4.0 trouxe inovações nos sistemas e negócios, apresentando novos desafios relacionados à gestão de riscos e ciberataques. As unidades de saúde não estão imunes a estas mudanças, e o conceito de "Hospital 4.0" [80] faz parte de nosso cotidiano. Tecnologias como IoT, inteligência artificial, big data, impressão 3D e realidade virtual estão a transformar estas instituições, permitindo estratégias de prevenção, manutenção e gestão de saúde mais eficazes.

A capacidade de fornecer atendimento personalizado e ter um conhecimento abrangente do histórico de saúde de um paciente torna a saúde um alvo atraente para indivíduos mal-intencionados ou cibercriminosos. Estes dados podem ser explorados de várias maneiras, desde prejudicar o tratamento até a negação de cuidados. Além disso, estas informações podem ser usadas como moeda de troca para aceder a serviços médicos caros, equipamentos ou benefícios fraudulentos de seguros de saúde, tornando-as altamente valiosas na dark web[4].

Os sistemas IoT partilham muitas das vulnerabilidades de segurança dos sistemas de rede convencionais, uma vez que a maioria das comunicações é baseada no protocolo IP. Com a crescente utilização desses dispositivos no nosso cotidiano, é fundamental considerar como proteger as informações recolhidas, uma vez que eles estão cada vez mais expostos a ameaças e ataques.

[4] Conjunto de redes encriptadas, intencionalmente escondidas da internet comum, visível apenas através de um browser específico

As constantes ameaças à segurança, destacadas na comunicação social, nas redes sociais e em fóruns online, colocam as equipas locais de tecnologia da informação sob constante pressão e alerta.

É importante ressaltar que as tecnologias estão a evoluir constantemente, recolhendo cada vez mais informações, o que atrai cibercriminosos em busca destes dados valiosos.

Diariamente, scripts são lançados online para fazerem um varrimento á web mundial em busca de novos dispositivos, que podem ser uma porta de entrada para redes locais. Um exemplo disso é o portal Shodan [81] [82] que varre a internet e apresenta vários dispositivos expostos, segmentados por tipo e localização.

Dados financeiros e informações clínicas sempre foram e continuarão a ser alvos atraentes para cibercriminosos, devido à natureza sensível dessas informações. O acesso a dados financeiros pode enriquecer os cibercriminosos, enquanto o acesso a dados de saúde pode afetar diretamente a sobrevivência das pessoas.

A partir da análise realizada, foi criada a tabela 4, que pode ser considerada na implementação de dispositivos IoT em unidades de saúde. Isto ajuda a validar se os dispositivos atendem aos requisitos apresentados.

Inventariação	
	Inventariar o equipamento com um número interno
	Preenchimento da ficha de artigo/equipamento
Segurança física	
	Validar se o equipamento tem portas em funcionamento desnecessárias Ex: Usb, rj45, rs232
	Validar se o equipamento tem interfaces em funcionamento desnecessários Ex: Câmara, microfone, coluna
	Validar se o equipamento tem botão de reset facilmente acessível ou permite reposição de definições de fábrica
	Validar se o equipamento possibilita o armazenamento de dados externos
	Validar se o equipamento fica exposto ou facilmente acessível fisicamente

Acessos e privacidade	
	Validar se o equipamento valida o uso de passwords fortes
	Validar se o equipamento é suscetível a ataques XSS, SQLi ou CSRF
	Alterar a senha por defeito na primeira configuração
	Validar se após tentativas de login inválido o sistema bloqueia o utilizador
	Validar se o utilizador é notificado de acessos indevidos
	Validar se o utilizador é notificado aquando da alteração da password
	Ativar a autenticação multi-fator
	Colocar uma password única por equipamento
	Atribuir credenciais de acesso diferentes por utilizador
	Validar se a recuperação de password tem mecanismos seguros
	Validar se as passwords ficam encriptadas na base de dados
	Criar utilizadores com acessos mínimos e diferenciados
	Validar se as contas de utilizador podem ser enumeradas remotamente
	Validar se o equipamento não envia os dados para outro local (fuga de informação)
	Verificar se o equipamento recolhe apenas os dados fundamentais para a funcionalidade do equipamento
	Verificar se os dados pessoais são encriptados e protegidos
	Validar se apenas pessoas autorizadas têm acesso aos dados recolhidos do equipamento
	Validar se o equipamento é blindado e se contempla mecanismos de Reverse Engineering

Configurações insuficientes de segurança	
	Validar se o equipamento utiliza protocolos como SSL e TLS para encriptar as comunicações
	Validar se o equipamento utiliza protocolos HL7 ou DICOM
	Validar se o equipamento utiliza padrões de criptografia opensource e evita o uso de protocolos de encriptação proprietários
	Validar se o equipamento garante o registo de eventos de segurança
	Validar se o equipamento notifica os utilizadores dos eventos de segurança
Serviços de rede	
	Verificar se o equipamento é vulnerável a ataques de buffer overflow, fuzzing ou DDoS
	Verificar se o equipamento bloqueia os serviços críticos se estes forem comprometidos ou atacados
	Colocar o equipamento numa VLAN especifica
	Validar se o equipamento permite ligação por VPN ou acesso remoto
	Atribuir uma entrada especifica na firewall para o equipamento
	Analisar se o tráfego enviado é encriptado
	Verificar se existem portos abertos que não sejam necessários
	Verificar se o equipamento deteta ou bloqueia pedidos de atividade anormal
Software / Firmware	
	Verificar se o equipamento disponibiliza atualizações periódicas
	Verificar se o equipamento possibilita ligações simultâneas
	Verificar se a atualização é assinada digitalmente
	Verificar o change log das atualizações
	Subscrever alertas de atualizações no portal do fornecedor
Acompanhamento e formação	
	Validar se as equipas foram envolvidas em todos os processos (desde a compra à instalação)
	Ministrar formação aos utilizadores dos equipamentos
	Ministrar formação de cibersegurança aos restantes funcionários periodicamente
	Efetuar testes de penetração com regularidade
	Validar se existem falhas conhecidas neste tipo de equipamentos
	Efetuar uma monitorização continua, classificando as vulnerabilidades encontradas
	Subscrever alertas de vulnerabilidades para o equipamento

Tabela 4– Check list para implementação de equipamentos IoT em Unidades de Saúde

Após análise da tabela 4, onde se apresenta um conjunto de boas práticas a ter em conta aquando da implementação de equipamentos IoT em unidades de saúde, procedeu-se á análise dos principais aspetos abordados:

5.1. Inventariação

Um dos primeiros passos essenciais na gestão da segurança das unidades de saúde é a realização de uma inventariação abrangente. Isso implica compreender os riscos de segurança associados aos equipamentos conectados à rede. Para realizar essa tarefa de forma eficaz, as equipas e profissionais dos departamentos de tecnologia da informação das organizações de saúde devem classificar cuidadosamente os dispositivos sensíveis da rede, identificando aqueles de maior importância, a fim de priorizar esforços em caso de ameaças à segurança.

Existem diversas ferramentas e programas disponíveis para realizar a inventariação dos ativos de rede, bem como programas que monitorizam continuamente a rede em busca de novos dispositivos ativos. À medida que o processo de inventariação avança, é fundamental agrupar e ordenar os dispositivos de acordo com o impacto que podem causar na rede. Dispositivos com alto impacto ou que representem um risco maior devem ser destacados e receber um acompanhamento mais próximo, garantindo assim o controlo adequado sobre eles.

A lista de equipamentos deve ser atualizada sempre que um novo dispositivo é adicionado à rede ou quando ocorre a substituição de um dispositivo existente. A simples substituição de um dispositivo não garante que o firmware ou a versão de software presentes sejam idênticos aos do dispositivo antigo que foi substituído.

As listas de equipamentos devem conter os seguintes campos:

- Nome do equipamento
- Número de série
- Modelo
- Endereço IP
- Portas abertas
- Versão de software
- Versão de firmware
- Localização física

- Serviço ao qual está vinculado
- Data de instalação do equipamento
- Data da última verificação de atualizações
- Vulnerabilidades conhecidas
- Risco/impacto

Além destes campos essenciais, é possível enriquecer a lista com informações adicionais, como modelo do processador, capacidade de memória, protocolo de comunicação, sistema operativo, VLAN na qual está inserido, campo de observações e outros detalhes pertinentes.

5.2. Segurança física

Quando se solicita a conexão de um equipamento à rede, é crucial realizar uma avaliação abrangente do equipamento em termos físicos, examinando-o minuciosamente. Esta análise visa certificar-se de que o equipamento está em conformidade com as especificações originais do fabricante e, ao mesmo tempo, auxiliar no processo de inventário, uma vez que envolve uma investigação aprofundada de seu hardware.

Todas as funcionalidades que não sejam estritamente necessárias devem ser desativadas, tais como câmaras, microfones, portas RS232 ou portas USB. No caso de existirem portas físicas que não estejam em uso, é igualmente importante desabilitá-las.

É essencial restringir o acesso físico ao equipamento, impedindo a ocorrência de intrusões indesejadas, como, por exemplo, a restauração para reset de fábrica ou o uso de passwords por defeito. Deve ser feita uma análise detalhada do equipamento para verificar a presença de qualquer botão que possa realizar ações desse tipo. Se identificado, pode ser necessário proteger o equipamento, vedando o acesso. Isto pode ser alcançado por meio do uso de caixas de segurança com cadeados ou posicionando os equipamentos em locais inacessíveis.

Sempre que viável, a criptografia deve ser ativada, mas, no momento da aquisição ou compra, é aconselhável dar preferência a equipamentos que já criptografem todos os dados transmitidos.

Os equipamentos devem contar apenas com as saídas físicas estritamente necessárias, seja em termos de portas USB ou slots para cartões SD. Todas as portas não utilizadas devem ser

inutilizadas ou ter o seu acesso vedado. Caso não seja possível bloquear o acesso por meio de software ou hardware, esta limitação deve ser tratada fisicamente.

5.3. Acessos e privacidade

Estes equipamentos IoT devem possuir autenticação forte por defeito, devendo ser avaliado a implementação do uso de autenticação multi-fator (2FA) e a utilização de certificados seguros para as credenciais de acesso. Deve-se assegurar que qualquer codificação do portal web (local ou na cloud) ou no aplicativo móvel seja programado impedindo o uso de senhas fracas, incluindo mecanismos de bloqueio de conta caso existam múltiplas tentativas de acesso errado. A senha deverá expirar após um período previamente especificado se o utilizador não for efetuando um acesso pontual e deverá ser sempre solicitado a alteração do nome de utilizador e a senha aquando da primeira utilização do dispositivo IoT.

As senhas de acesso administrativo não devem ser utilizadas para outros tipos de acesso, delineando o respetivo impacto aquando do reset de fábrica. Os equipamentos devem ter acesso somente a uma interface local e deverá ser registado uma senha única por dispositivo. A utilização de multiutilizadores deve ser contemplada, elencando as funções para cada cenário e os respetivos níveis de acesso devem estar detalhados.

Os mecanismos de recuperação de senhas devem ser realizados sempre através do suporte multi-fator, seja por mensagem de texto (sms), por chamada, por gerador de códigos ou por mail desde que validado por um pin previamente definido.

As passwords locais e remotas deverão ser atualizadas para passwords fortes e de difícil memorização, sendo que cada equipamento deverá ter uma password distinta. Aconselha-se o uso de um gestor de passwords para guardar as passwords dos variados equipamentos de forma encriptada. Este gestor de passwords deverá ficar numa máquina isolada da rede, e sem ligação á internet para que não seja comprometida. A título de exemplo poderá ser utilizado um telemóvel em modo de voo, com a aplicação instalada, e este equipamento deverá ser guardado em cofre próprio na instituição.

O equipamento deverá validar se a password é robusta, se tem mais do que 15 caracteres, não contem palavras conhecidas do dicionário e se é composta por números, símbolos, letras maiúsculas e letras minúsculas, aumentando assim o grau de complexidade da password.

Existem gestores de password que possuem mecanismos para gerar este tipo de password, únicas e com elevado grau de complexidade.

Sempre que possível deverá ser dada preferência a compra de equipamentos IoT que possibilitem utilizar a autenticação de vários fatores, tipo autenticação 2FA.

Os acessos deverão ser atribuídos apenas quando é necessário, de forma a controlar as permissões de cada dispositivo, pelo que deverão ser criados diversos utilizadores com diversas camadas de operação.

Deverão ser descartados equipamentos que dependem de aplicações ou serviços com pouca segurança e sem privacidade.

Devem ser implementadas políticas de bloqueio, ou desativação de contas de utilizador quando são feitos ataques de brute force ou após um número razoável de tentativas de login inválidas.

Sempre que existir uma alteração de senha os utilizadores deverão ser notificados via email, e deverá ser enviado um código de validação para um dispositivo móvel para validar a alteração da senha. Estas alterações deverão ser guardadas em logs, ficando com um histórico de acessos para todos os eventos de segurança.

As credenciais de autenticação armazenadas em base de dados remotas ou nos próprios equipamentos, devem ser encriptadas, utilizando métodos de criptografia numa primeira instância com um hash, e se possível um hash com um salt para aumentar a complexidade da cifra. Os dados pessoais transmitidos também não deverão ser exceção pelo que os dados em transito deverão ser sempre encriptados.

Deve ser garantido uma credencial única de acesso por utilizador, descartando o usual admin para a gestão do equipamento. Cada utilizador deverá ter um login diferente, e cada login poderá ter permissões distintas, ou só de leitura, ou só escrita, ou de acesso total.

Aquando da criação do utilizador deverá ficar evidenciado quais os acessos que efetivamente necessita, pelo que os acessos deverão ser criados de forma minimalista e adicionado posteriormente mais permissões se os atribuídos inicialmente não se ajustarem com o que é expectável.

Sempre que existirem alterações de passwords ou acessos indevidos deverão ser emitidos alertas, por email ou sms para o lesado, informando por exemplo que em determinado dia e em determinado IP a password foi alterada sendo possível atuar prontamente.

Os equipamentos IoT devem possuir protocolos de segurança e criptografia atualizada e o portal web deverá ter a capacidade de utilizar o protocolo HTTPS para proteger as informações enviadas na comunicação ou partilha de informação.

O protocolo HTTPS é igual ao protocolo HTTP, no entanto, esta variante utiliza certificados para proteger as comunicações entre o servidor e o cliente e vice-versa, colocando assim mais uma camada de proteção, pelo que é fulcral para evitar ataques do tipo man-in-the-middle.

A monitorização da segurança dos equipamentos deverá estar presente para reduzir possíveis impactos de vulnerabilidades e deverão ser efetuados testes a todas as vertentes webs, testando as vulnerabilidades XSS, SQLi e CSRF.

A distribuição das correções de vulnerabilidades identificadas e as atualizações destas vulnerabilidades através de mecanismos eficazes não deverão modificar as configurações de utilizadores previamente configurados, nem deverão fornecer a capacidade de autorizar ou não futuras atualizações automáticas.

A recolha de dados deve ser limitada ao que for razoavelmente útil para a funcionalidade e finalidade a que se destina, pelo que devem ser avaliados os dados que realmente são necessários salvaguardando apenas os que interessam, encriptando sempre dados de cariz pessoal, ou com informações clínicas.

De forma a precaver a fuga da informação, deverá ser garantido que o equipamento não envia uma cópia dos dados para outro local, assim como deverão estar disponíveis apenas os portos estritamente necessários á atividade, devendo ser barrados outros portos na firewall de forma a mitigar este problema.

Devem também ser efetuados testes de penetração, validando se é possível enumerar os utilizadores registados, assim como as referidas passwords de cada um, tomando as medidas necessárias para evitar a exploração desta vulnerabilidade, agilizando com o fornecedor uma medida corretiva caso seja necessário.

A política de retenção de informação deverá ser de conhecimento público e disponibilizada a todos os intervenientes antes da utilização do dispositivo, pelo que deverá ser possível ao

utilizador recusar qualquer política imposta sobre a partilha de informação, notificando-o dos impactos que poderá ter no funcionamento do IoT.

A anonimização de dados deverá ser garantida cumprindo com a legislação em vigor no que diz respeito ao RGPD - Regime Geral de Proteção de Dados. De salientar que deve ser garantido que apenas utilizadores autorizados tenham acesso a informações pessoais, sendo que o utilizador em questão deverá ser notificado deste acesso sempre que ocorra um evento que assim o justifique.

O equipamento deverá garantir mecanismos de blindagem que inviabilizem o reverse engineering ou a engenharia reversa, precavendo que o código seja extraído diretamente das placas de memória existente no interior do equipamento. O código ao ser extraído e ao ser analisado poderá ser fruto de uma análise mais profunda por cibercriminosos, pelo que tentarão a todo o custo encontrar pontos de entrada que poderão ser explorados futuramente.

5.4. Configurações insuficientes de segurança Acessos e privacidade

A eficiência das comunicações de eventos de segurança é essencial, e os utilizadores devem ser notificados sempre que esses eventos ocorram, seja por email, mensagem de texto ou outro meio de comunicação à sua escolha. Além disso, a padronização do idioma por utilizador deve ser suportada, permitindo a seleção da linguagem preferida.

As notificações principais devem ser enviadas quando houver alterações no acesso, como alterações de password ou tentativas de login incorretas. De evidenciar que todos os demais eventos de segurança deverão ficar acessíveis ao utilizador em local próprio, podendo ser consultado a qualquer instante, disponibilizando a que horas, determinado endereço acionou uma dada ação ou qual a ocorrência efetuada.

Para proteger as comunicações, o equipamento deve utilizar protocolos SSL (Secure Socket Layer) e TLS (Transport Layer Security) para criptografar as informações transmitidas. Estes protocolos garantem a segurança na troca de dados entre aplicações, servidores e clientes, usando chaves de criptografia baseadas no conteúdo do tráfego.

Os dispositivos IoT devem adotar padrões de criptografia baseados em código aberto, evitando o uso de protocolos proprietários de criptografia. A criptografia baseada em código

aberto permite a colaboração global da comunidade de programadores, resultando em melhorias contínuas e maior segurança. Estes tipos de criptografia são continuamente testados por computadores poderosos em todo o mundo, criando padrões robustos e difíceis de violar ou decifrar.

Para garantir a interoperabilidade global, os dispositivos IoT que lidam com dados clínicos devem transmitir informações de acordo com normas de comunicação reconhecidas, como HL7 ou DICOM. Essas normas são amplamente utilizadas em todo o mundo, garantindo a integridade e consistência das informações compartilhadas. Elas estabelecem regras que permitem que as informações sejam partilhadas e interpretadas de maneira consistente, facilitando a comunicação entre diferentes dispositivos usando a mesma linguagem.

5.5. Serviços de Rede

A correta segmentação da rede desempenha um papel fundamental na gestão da segurança de dispositivos IoT, permitindo restringir o acesso e a comunicação entre diferentes camadas, categorizando os equipamentos com base em níveis, dados e grupos específicos. Esta abordagem estabelece limites que controlam o fluxo de informações, facilitando a identificação de comunicações suspeitas.

A segmentação da rede desempenha um papel importante na prevenção do roubo de informações e na propagação de malware, proporcionando confiança às equipas de tecnologia da informação locais para adotar novas soluções de dispositivos IoT. Ela adiciona uma camada adicional de segurança e proteção de dados sem comprometer o desempenho e a confiabilidade.

A segmentação da rede permite isolar ameaças em camadas específicas, evitando, por exemplo, o roubo de dados clínicos ou a propagação de criptografia de malware pela rede. Ao separar dados clínicos do restante da rede, as equipas de TI podem monitorizar o tráfego com mais eficácia e detetar atividades suspeitas que possam indicar um dispositivo comprometido.

É importante considerar cuidadosamente a segmentação da rede, especialmente quando dispositivos diferentes partilham a mesma rede, como uma impressora e um monitor de sinais vitais. Limitar o acesso de forma que dados sensíveis não se misturem com dados comuns é essencial.

A criação de VLANs é uma maneira eficaz de implementar a segmentação da rede, restringindo o acesso à internet ou a outras redes externas apenas ao estritamente necessário. Antes de colocar dispositivos IoT em produção, é crucial avaliar o impacto que eles terão na rede.

Dispositivos IoT devem ser colocados numa rede separada com firewall e monitorização de tráfego. Além disso, é recomendável preferir dispositivos que suportem o uso de VPN para gestão e monitorização, evitando conexões não autorizadas à rede Wi-Fi.

O acesso via VPN adiciona uma camada adicional de segurança, criando um túnel virtual que protege a comunicação contra invasões e garante a privacidade dos dados transmitidos.

Todas as exceções à segmentação da rede devem ser claramente documentadas na tabela de inventário para mitigar riscos e evitar exposições não planeadas de dispositivos com vulnerabilidades conhecidas. A utilização de firewalls de perímetro para proteger todas as interfaces da rede é recomendada, permitindo apenas o tráfego necessário para o funcionamento dos dispositivos.

O futuro do IoT foca-se em tornar uma rede de equipamentos autónomos que podem interagir uns com os outros e tomar decisões inteligentes sem intervenção humana. É nesta fase que o blockchain pode ajudar esta tecnologia a dar o salto e a formar uma base sólida que suportará a transação das comunicações de forma mais segura e única.

O blockchain pode ser usado para preservar e proteger dados no âmbito do IoT uma vez que poderá ser possível analisar todas as transações efetuadas.

A encriptação é um dos eixos fundamentais para que esta tecnologia vingue e ganhe a credibilidade que tem sido abalada ultimamente. Ao proceder-se à encriptação dos dados, passará a ser mais difícil analisar o teor das comunicações, garantido uma confidencialidade nas transações efetuadas.

O desempenho dos equipamentos deverá ser monitorizado constantemente para validar se está a efetuar apenas a função que lhes compete, verificando se não existe consumo de tráfego anormal ou se a informação está a ter o destino esperado.

Todo o tráfego gerado pelos equipamentos IoT deverá ser analisado, com programas tipo o Wireshark, ou Tcpdump para perceber se o equipamento está a encriptar as comunicações e se está a recolher ou a enviar o estritamente necessário.

Deverá também ser analisado o tráfego que o equipamento recebe e transmite e verificar se existem portas no software abertas que podem permitir o controle remoto.

Poderá ser efetuado uma bateria de testes de forma a precaver os ataques de buffer overflow, de fuzzing ou de negação de serviço. Estes ataques têm como principal objetivo tornar o equipamento indisponível, pelo que o equipamento deverá saber interpretar que está a ser alvo de um ataque e deverá bloquear serviços críticos se estes forem comprometidos, enviando alarmística para a equipa local de sistemas de informação de forma a esta agir em conformidade o mais rapidamente.

5.6. Software e firmware

Manter um equipamento IoT atualizado, tanto em termos de software quanto de firmware, é fundamental para evitar que potenciais invasores explorem falhas conhecidas. É crucial manter um controlo rigoroso das versões instaladas, documentando-as adequadamente na ficha de cada equipamento.

O controlo de versões deve ser um processo registado e ativado, e é recomendável subscrever alertas junto aos fornecedores para receber notificações automáticas por e-mail sempre que uma nova atualização estiver disponível, mantendo assim as equipas locais de sistemas de informação informadas.

É essencial ter um processo de monitorização ativa e um fluxo interno bem estabelecido para verificar regularmente se existem novas atualizações e patches de segurança disponíveis, a fim de prevenir possíveis problemas de segurança na rede.

Antes de realizar uma atualização, é fundamental analisar minuciosamente o "change log", um arquivo fornecido pelo fabricante que lista todas as alterações feitas desde a última atualização. Isso ajuda a garantir que as atualizações planeadas estejam alinhadas com os objetivos e não prejudiquem o desempenho pretendido.

Tanto o firmware quanto o software devem ser mantidos atualizados com as versões mais recentes, pois os fabricantes geralmente corrigem vulnerabilidades e disponibilizam novos firmwares para resolver problemas de segurança. As atualizações automáticas devem ser ativadas, mas é aconselhável também subscrever alertas junto dos fabricantes para garantir uma gestão mais eficiente. É importante ler com atenção as informações fornecidas pelos

fabricantes, pois algumas atualizações podem impactar negativamente a segurança, alterando algo inesperado.

Todas as atualizações devem ser assinadas digitalmente para garantir que não comprometam a segurança da rede, evitando a instalação de firmwares adulterados ou manipulados por terceiros.

Equipamentos que não recebem mais atualizações devem ser identificados e, quando possível, retirados de funcionamento ou isolados na rede. Estes dispositivos podem ser alvos atraentes para cibercriminosos em busca de vulnerabilidades conhecidas, uma vez que o acesso a eles provavelmente permanecerá ativo sem correções.

Além disso, a subscrição de alertas nos portais dos fornecedores deve ser ativada para receber notificações automáticas sobre vulnerabilidades ou novas atualizações disponíveis para dispositivos específicos.

Os equipamentos IoT devem ser projetados para permitir conexões simultâneas sem afetar o funcionamento regular. É essencial garantir que os dados enviados e recebidos cheguem ao destinatário correto, independentemente do número de clientes conectados ao equipamento.

Por fim, os fabricantes deveriam adotar o SSDLC (Secure Software Development Lifecycle) como prática padrão, incorporando modelos de ameaças para prevenir ataques e garantir a segurança durante o desenvolvimento de software e firmware.

5.7. Acompanhamento e formação

O acompanhamento e o envolvimento das equipas de informática são fulcrais em todas as fases. Estas equipas deverão ser integradas numa primeira instância para efetuar o levantamento das necessidades de cada equipamento, sugerindo o melhor artigo a comprar, considerando sempre a segurança como ponto fundamental.

Na fase da implementação deverão ser envolvidas também as equipas no terreno, colocando o equipamento em produção, procedendo aos testes necessários, e á respetiva inventariação.

A cibersegurança está em constante evolução, pelo que as equipas de tecnologias necessitam de estar permanentemente atualizadas sobre as ameaças mais recentes. Ao dotar estes profissionais e estas equipas de formação especifica será possível criar melhores defesas e

também uma maior consciencialização para os restantes funcionários sobre os ataques e fraudes que poderão acontecer.

A cibersegurança exige um trabalho diário de equipa com todos os membros da organização envolvidos na identificação de possíveis vulnerabilidades ou ameaças, alertando os demais funcionários envolvidos para não serem vítimas de qualquer tipo de ataque, consciencializando os profissionais para os ataques de engenharia social. Os ataques de engenharia social têm vindo a ganhar adeptos, pelo que um cibercriminoso ao conseguir obter informação adicional de um determinado funcionário, pode ajustar o seu espectro de ação com base na informação recolhida.

De forma a criar uma rede segura, e um ecossistema interno isento de riscos, as equipas de tecnologias de informação das mais variadas unidades de saúde, devem saber lidar com as vulnerabilidades que vão encontrando nos equipamentos que vão instalando e deverão ser equipas pró-ativas, jogar sempre na defensiva, pelo que deverão estar em constante formação.

A formação deverá ser essencialmente em proteção e em medidas de defesa, dado que neste tipo de área é muito difícil prever os problemas que poderão advir. Todos os dias existem novas formas, novas táticas, novas técnicas e novos modos de operação.

A forma como se reage ou atua depois de um ciberataque também deverá ser equacionado, e os profissionais deverão estar consciencializados para esta realidade.

A formação deverá incidir sobre ataques conhecidos, que já tenham ocorrido em outras instituições e assim aprender com os erros cometidos por outras equipas melhorando o know-how interno.

Os profissionais que utilizem a rede interna deverão ser sensibilizados para este tipo de risco, pelo que periodicamente poderão ser feitos pequenos testes, como por exemplo o envio de emails falsos tipo phishing, de forma a identificar as fraquezas internas e a poder direcionar a formação a um grupo de funcionários restritos onde a sua cultura de defesa ou de cibersegurança seja mais urgente. É comum os funcionários internos caírem em esquemas de engenharia social, nomeadamente provenientes de emails, que por sua vez acionam a instalação de software malicioso colocando em risco a restante rede.

Alguns equipamentos IoT na sua génese necessitam de software extra para se poderem configurar, pelo que deverá existir uma cultura de defesa e um nível de desconfiança que faça sempre duvidar qualquer tipo de ação anómala.

Deverá ser ministrada formação aos utilizadores da rede, uma vez que cada vez mais ocorrem ataques de engenharia social, sendo os próprios funcionários os intervenientes nos ataques, assim é fulcral educar os utilizadores dos equipamentos sobre os riscos de segurança e os problemas que advém da utilização de equipamentos IoT.

É fundamental que as equipas locais fomentem uma cultura severa e rígida ao nível de segurança, alegando que os equipamentos IoT são provavelmente mais vulneráveis do que os dispositivos tradicionais apresentando evidencias, provas e factos.

O amplo leque de funcionários deve ser sensibilizado para que inadvertidamente possam facilmente cair num ataque de phishing ou num ataque de engenharia social. Esta sensibilização pode ser feita com formação, e campanhas internas de divulgação de boas práticas.

Aquando da sua implementação, é fundamental que se efetuem testes funcionais para validar a integridade e o desempenho do dispositivo.

Os testes de penetração (pentest) são muito uteis para dar às equipas locais de tecnologias de informação quais as vulnerabilidades que um dado equipamento detém, assim como perceber onde atuar para mitigar problemas que possam causar muito impacto.

Os testes de penetração exploram as fraquezas já conhecidas, existentes em determinados equipamentos. Estes testes também permitem identificar se os demais equipamentos podem levar a violação de informação sensível ou a atividades maliciosas.

Após um teste deve ser sempre gerado um relatório onde fica um resumo das vulnerabilidades encontradas e as respetivas formas de mitigação.

Deverão ser feitos testes de penetração com regularidade para encontrar novas vulnerabilidades nos equipamentos, no entanto é de salientar os limites impostos pela lei do cibercrime.

Com as vulnerabilidades encontradas, deverá ser classificado o equipamento com o respetivo risco que poderá trazer á instituição, pelo que estes dados deverão ficar de fácil consulta na ficha do equipamento.

A capacidade de testar um ataque e verificar como estão as equipas preparadas para uma ciberdefesa também é um ponto chave que deverá ser trabalhado. Este tipo de testes ajuda a melhorar o tempo de resposta a ataques e aumenta a eficiência na defesa, uma vez que existe uma maior consciencialização para os riscos e perigos a que estão sujeitos.

Apesar das demais medidas preventivas implementadas pelas organizações, estas ainda enfrentam variadíssimas falhas de segurança. Assim é fundamental a implementação de algoritmos de deteção de intrusões (IDS) e sistemas de prevenção contra invasões (IPS), software antivírus, firewall e um sistema de gestão e correlação de eventos de segurança (SIEM) para ajudar a detetar falhas de segurança no seu período inicial.

A deteção de falhas pode ser efetuada com testes de penetração, com pesquisa em páginas da atualidade e com o acompanhamento dos mais recentes CVE (Common Vulnerabilities and Exposures). Estas páginas são públicas e é possível subscrever alertas para receber email sempre que exista uma vulnerabilidade nova.

Também existem sites governamentais que podem ser consultados, como é o caso do Centro Nacional de Cibersegurança (CNC) que possuem informações atualizadas das ameaças mais comuns.

Depois de colocar em produção novos equipamentos é fundamental verificar se estes equipamentos colidem com outros e se colocam em risco algum outro equipamento.

É fundamental que se efetue uma monitorização continua de forma a encontrar novas vulnerabilidades nos equipamentos.

As vulnerabilidades encontradas deverão ser designadas ao equipamento onde foram encontradas, na folha de inventário, onde facilmente se poderá consultar todo o histórico do equipamento centralizando assim a informação num único local.

Deverá também ser usada uma escala de 0 a 10 para identificar o risco, sendo o risco baixo, médio, alto ou crítico em função do impacto que causa.

A vulnerabilidade deverá ser descrita, com um resumo do tipo de ataque possível e o seu possível impacto, devendo esta informação ficar centralizada, na ficha do equipamento aquando da sua inventariação.

5.8. Síntese

Neste capítulo, foi desenvolvida uma tabela que pode servir como guia para a implementação de equipamentos IoT em unidades de saúde. Essa tabela pode ser utilizada como uma lista de verificação contendo vários tópicos que precisam ser analisados e validados.

Este capítulo apresenta um conjunto de regras de boas práticas destinadas a orientar a implementação de equipamentos IoT, com o objetivo de proteger os dados críticos e sensíveis da organização.

Dentro dos tópicos fundamentais abordados ao longo deste capítulo, destaca-se a importância de uma inventariação precisa, detalhando os campos que devem ser preenchidos de forma a identificar cada equipamento de maneira inequívoca. Também enfatizamos a segurança física, destacando a necessidade de proteger e desabilitar portas ou periféricos que não estejam em uso.

Questões relacionadas com o acesso e a privacidade dos dados pessoais são discutidas, com foco especial na alteração das passwords por defeito e na configuração de alertas de segurança sempre que eventos críticos ocorrerem.

É abordada ainda a importância de configurar adequadamente as medidas de segurança, os serviços de rede e a necessidade de criptografar as comunicações.

Destaca-se a relevância das atualizações dos equipamentos, seguindo o acompanhamento e a necessidade de fornecer formação aos funcionários para conscientizá-los sobre a importância desses equipamentos.

As boas práticas apresentadas neste capítulo visam fornecer às unidades de saúde e às equipas de suporte de sistemas de informação um guia para a implementação eficaz de IoT, seguindo um conjunto de passos que, até agora, eram frequentemente realizados de forma ineficiente.

O desenvolvimento desta lista de verificação visa abordar as questões identificadas no capítulo 3, onde são discutidos os problemas associados aos diversos equipamentos IoT presentes em unidades de saúde. Isso permite que, após a leitura do capítulo 2, onde são apresentados os principais tipos de ataques, riscos e vulnerabilidades, as organizações estejam mais bem preparadas para lidar com esses desafios.

Para concluir este estudo, o próximo capítulo consolidará os temas discutidos aqui.

6. Conclusão

Os benefícios oferecidos pelos dispositivos IoT em unidades de saúde são inegáveis, fornecendo informações cruciais para pacientes, prestadores de serviços de saúde e profissionais da área. No entanto, as unidades de saúde devem estar cientes dos riscos e vulnerabilidades associados a estes dispositivos, garantindo que a prestação de cuidados de saúde não seja comprometida e que o desempenho e a confiabilidade não sejam afetados.

Os principais objetivos deste estudo focam-se em identificar e caracterizar os equipamentos IoT presentes em unidades de saúde, assim como na identificação os riscos e vulnerabilidades a que estão sujeitos.

É importante observar que os cibercriminosos podem identificar dispositivos mais vulneráveis e usá-los como ponto de entrada para comprometer a segurança de toda a rede. Dispositivos comuns que não recebem atualizações de firmware regularmente são particularmente suscetíveis a explorações.

Para mitigar esses riscos, foi desenvolvida uma lista de verificação contendo regras de boas práticas para a instalação de dispositivos IoT em unidades de saúde.

Atualmente, as arquiteturas IoT frequentemente priorizam a funcionalidade e a usabilidade em detrimento da segurança. Manter um equilíbrio entre segurança, funcionalidade e desempenho é um desafio, pois medidas de segurança rigorosas podem sobrecarregar dispositivos e prejudicar a experiência do utilizador. No entanto, a segurança não pode ser subestimada.

Embora seja impossível antecipar todos os possíveis ataques e vulnerabilidades, é essencial trabalhar proactivamente na proteção dos dispositivos IoT em unidades de saúde. Isso inclui atualizações regulares de firmware, rigorosas políticas de segurança, consciencialização dos utilizadores, uso de passwords seguras e encriptação.

A segurança é um desafio contínuo, e os padrões e práticas precisam ser constantemente atualizados. Também abordada a importância de lidar com ameaças internas, destacando a necessidade de monitorizar o comportamento dos funcionários.

Em resumo, os dispositivos IoT em unidades de saúde oferecem oportunidades significativas, mas também apresentam desafios complexos de segurança. Através da adoção de boas práticas e da conscientização contínua, as unidades de saúde podem maximizar os benefícios desses dispositivos enquanto protegem a privacidade e a integridade dos dados dos pacientes.

6.1. Trabalho Futuro

Para futuros desenvolvimentos, é fundamental expandir estas diretrizes de boas práticas para abranger outros dispositivos de saúde que não foram abordados neste documento ou que possam surgir no mercado posteriormente.

Além disso, seria importante investigar a viabilidade de conduzir análises forenses nos dispositivos IoT comprometidos após um ataque. Isso permitiria compreender melhor a extensão do comprometimento e as possíveis ações de recuperação.

Outro ponto importante que poderá ser explorado no futuro é a utilização da tecnologia blockchain para a partilha segura de informações e proteção dos dados clínicos de cada paciente. O blockchain pode desempenhar um papel crucial na garantia da integridade e confidencialidade dessas informações sensíveis.

É fundamental também estabelecer um plano de resposta a incidentes bem estruturado, garantindo a continuidade dos negócios em caso de ataques ou interrupções nos sistemas. Ter procedimentos claros para lidar com situações adversas é essencial para manter a segurança e a eficácia das operações.

Por último, seria a criação de uma plataforma web dedicada à gestão de dispositivos IoT, especificamente projetada para atender às necessidades deste cenário. Essa plataforma poderia oferecer recursos como avaliação automática de riscos e análise de vulnerabilidades, tornando-a aplicável em diversos contextos de negócios relacionados à Indústria 4.0.

7. Anexos

Segue-se página web, criada no WordPress, alojada em servidor interno com o objetivo de sensibilizar os utilizadores da ULS. Aqui, os colaboradores poderão encontrar um manual de boas práticas em cibersegurança, definições e conceitos de cibersegurança, estar a par das ocorrências (notícias em cibersegurança) do momento, bem como colocar questões e realizar testes de conhecimento.

ULSG SEGURA

Página Inicial Manual de Boas Práticas Guia de Cibersegurança Conteúdos

ULSG SEGURA

Página Inicial Manual de Boas Práticas Guia de Cibersegurança Conteúdos

Guia de cibersegurança

- O que é a Cibersegurança?
- Que tipos de ciberataques existem?
- Que consequências pode ter um Ciberataque?
- Quem são os atacantes?
- O que é a Engenharia Social?
- O que é o phishing?
- O que é o vishing? E o smishing?
- O cadeado no site significa que este é seguro?
- Todas as redes wi-fi são seguras?
- Como criar uma password forte?
- Como comprar online de forma segura?
- Qual é a relação da Cibersegurança com o RGPD?
- O que é formjacking?

Referências bibliográficas

[1] N. I. of Standards e Technology, *NIST*, Website, visitado em 09-2023. URL: https://www.nist.gov/.

[2] NIST, «Framework for Improving Critical Infrastructure Cybersecurity», 2018. doi: 10.6028/NIST.CSWP.04162018.

[3] E. Parliament, *Directive on security of Network and Information Systems*, Website, visitado em 09-2023. URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333.

[4] ENISA, *Áreas de atuação NIS*, visitado em 09-2023. URL: https://www.enisa.europa.eu/topics/nis-directive/nis-visualtool.

[5] RNCSIRT, *Rede Nacional CSIRT*, Website, visitado em 09-2023. URL: https://www.redecsirt.pt/.

[6] CIS, *Center for Internet Security (CIS)*, Website, visitado em 09-2023. URL: https://www.cisecurity.org/controls.

[7] *CIS Controls v8*, visitado em 09-2023. URL: https://www.cisecurity.org/insights/white- papers/cis- controls- v8- privacy- companionguide-portuguese-translation.

[8] Integrity, *ISO 27001 - Sistema de Gestão de Segurança da Informação*,Website, visitado em 09-2023. URL: https://www.27001.pt/.

[9] ISO, *ISO/IEC 27001 - INFORMATION SECURITY MANAGEMENT*, Website, visitado em 09-2023. URL: https://www.iso.org/isoiec- 27001-information-security.html.

[10] S. N. V. (Schweizerische, «Information technology-Security techniques-Information security management systems-Requirements. ISO/IEC International Standards Organization.», website visitado em 09/2023. URL: https://www.iso.org/standard/27001.

[11] E. Ramos, E. Cordeiro, G. Martins, N. Silva e E. Duarte, *Orientações para implementação do Sistema de Gestão de Segurança da Informação com base na ISO 27001 e o Ciclo PDCA. In FatecSeg-Congresso de Segurança da Informação, website, visitado em 09/2023. URL: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/34*.

[12] ISO, *ISO27701*, Website, visitado em 09-2023. URL: https://www.27701.pt/.

[13] APCER, *APCER - ISO27701*, Website, visitado em 09-2023. URL: https://www.apcergroup.com/pt/certificacao/pesquisa-de-normas/1571/isoiec-27701?highlight=WyJpc28iLCJpc28ncyIsImllYyIsMjc3MDEsImlzbyBpZWMiLCJpc28gaWVjIDI3NzAxIiwiaWVjIDI3NzAxIl0=.

[14] CNCS, *Roteiro das Capacidades Mínimas para a Cibersegurança*, visitado em 09-2023. URL: https : / / www . cncs . gov . pt / docs / cncs - roteiro - capacidades-minimas-ciberseguranca.pdf.

[15] CNCS, *Quadro Nacional de Referência para a Cibersegurança*, visitado em 09-2023. URL: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf.

[16] G. D. P. i. c. 2. Regulation, visitado em 09-2023. URL: https://gdprinfo.% 20eu..

[17] CNCS, *Regime Jurídico*, visitado em 09-2023. URL: https://www.cncs.gov. pt/pt/regime-juridico/.

[18] D.-L. n.º 65/2021, *Decreto-Lei n.º 65/2021*, Documento, visitado em 09-2023. URL: https://dre.pt/dre/detalhe/decreto-lei/65-2021-168697988.

[19] R. I. Hdowkfduh et al., "Survey of Smart Healthcare Systems using IOT," vol. 6, pp. 508–513.

[20] Health 4.0: Applications, Management, Technologies and Review, visitado em 04/2023. URL: https://www.academia.edu/38361992/Health_4_0_Applications_Management_Technologies_and_Review.

[22] A. j G. & Co, "Medical Device Cybersecurity, regulatory Oversight & Insurance," visitado em 04/2023. URL: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.

[23] Swati Khandelwal, "Medtronic's Implantable Defibrillators Vulnerable to Life-Threatening Hacks", visitado em 04/2023. URL: https://thehackernews.com/2019/03/hacking-implantable-defibrillators.html.

[24] E. McMahon, R. Williams, M. El, S. Samtani, M. Patton, and H. Chen, "Assessing medical device vulnerabilities on the Internet of Things," 2017 IEEE Int. Conf. Intell. Secur. Informatics Secur. Big Data, ISI 2017, pp. 176–178, 2017.

[25] H. Zhang, J. Li, B. Wen, Y. Xun, and J. Liu, "Connecting intelligent things in smart hospitals using NB-IoT," IEEE Internet Things J., vol. 5, no. 3, pp. 1550–1560, 2018.

[26] H. Choi, N. Kim, and H. Cha, "6LoWPAN-SNMP: Simple network management protocol for 6LoWPAN," 2009 11th IEEE Int. Conf. High Perform. Comput. Commun. HPCC 2009, pp. 305–313, 2009.

[27] J. Hui and A. R. Corporation, "RFC 6282: Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," pp. 1–24, 2011.

[28] T. Winter, P. Thubert, A. R. Corporation, and R. Kelsey, "RFC 6550: IPv6 Routing Protocol for Low-Power and Lossy Networks," pp. 1–157, 2012.

[29] S. C. Ergen, "ZigBee/IEEE 802.15. 4 Summary," UC Berkeley, Sept., vol. 10, p. 17, 2004.

[30] J. Decuir, "Bluetooth Smart Support for 6LoBTLE: Applications and connection questions," IEEE Consum. Electron. Mag., vol. 4, no. 2, pp. 67–70, 2015.

[31] T. Y. Wu and W. T. Lee, "The research and analysis for rear view transmission based on ieee 802.11 wireless network," Proc. - 2014 10th Int. Conf. Intell. Inf. Hiding Multimed. Signal Process. IIH-MSP 2014, no. Ieee 802, pp. 646–649, 2014.

[32] S. S. Park, "An IoT application service using mobile RFID technology," Int. Conf. Electron. Inf. Commun. ICEIC 2018, vol. 2018-Janua, pp. 1–4, 2018.

[33] ECMA International, "Near Field Communication - Interface and Protocol (NFCIP-1)," no. June, p. 52, 2013.

[34] W. Rzepecki, L. Iwanecki, and P. Ryba, "IEEE 802.15.4 thread mesh network - Data transmission in harsh environment," Proc. - 2018 IEEE 6th Int. Conf. Futur. Internet Things Cloud Work. W-FiCloud 2018, pp. 42–47, 2018.

[35] M. T. Buyukakkaslar, M. A. Erturk, M. A. Aydin, and L. Vollero, "LoRaWAN as an e-Health Communication Technology," Proc. - Int. Comput. Softw. Appl. Conf., vol. 2, pp. 310–313, 2017.

[36] J. R. E. Leite and P. S. Martins, "A Internet das Coisas (IoT) : Tecnologias e Aplicações," no. December 2017.

[37] D. Soni and A. Makwana, "A survey on mqtt: a protocol of internet of things (IoT)," Int. Conf. Telecommun. Power Anal. Comput. Tech. (Ictpact - 2017), no. April, pp. 0–5, 2017.

[38] M. B. Yassein, M. Q. Shatnawi, S. Aljwarneh, and R. Al-Hatmi, "Internet of Things: Survey and open issues of MQTT protocol," Proc. - 2017 Int. Conf. Eng. MIS, ICEMIS 2017, vol. 2018-Janua, pp. 1–6, 2018.

[39] K. H. e C. B. Zach Shelby, "RFC 7252: The Constrained Application Protocol (CoAP)," J. Chem. Inf. Model., vol. 53, no. 9, pp. 1689–1699, 2013.

[40] H. A. Khattak, M. Ruta, E. Eugenio, and D. Sciascio, "CoAP-based healthcare sensor networks: A survey," Proc. 2014 11th Int. Bhurban Conf. Appl. Sci. Technol. IBCAST 2014, pp. 499–503, 2014.

[41] R. T. Fielding et al., "RFC 2616: Hypertext Transfer Protocol," pp. 1–114, 1999.

[42] S. P. Jaikar and K. R. Iyer, "A Survey of Messaging Protocols for IoT Systems," Int. J. Adv. Manag. Technol. Eng. Sci., vol. 8, no. II, pp. 510–514, 2018.

[43] "HL7 international," visitado em 06-2023. URL: https://www.hl7.org/implement/standards/index.cfm?

[44] A. da República, "Diário da República, 1.a série — N.o 143 — 26 de julho de 2017," pp. 5688–5724, 2017.

[45] L. Janeiro, N. Matela, N. Oliveira, and P. Almeida, "Imagem Digital em formato DICOM: Conteúdo e Estrutura Digital Imaging in DICOM format: Its Content and Structure," pp. 73–79, 2011.

[46] O. Foundation, "Open industry specifications, models and software for e-health," 2011.

[47] Eleanor Dickinson, "Melbourne heart clinic hit by ransomware attack," ARN, visitado em 06-2023. URL: https://www.arnnet.com.au/article/658014/melbourne-heart-clinic-hit-by-ransomware-attack/.

[48] I. T. e R. Au-Yong, "SingHealth cyber-attack: How it unfolded," Straitstimes, visitado em 06-2023. URL: https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html.

[49] B. J. Sanborn, "UnityPoint Health System hit with cyberattack affecting 16,000 patients," Healthcare Finance News, 2018. [Online]. Available: https://www.healthcarefinancenews.com/news/unitypoint-health-system-hit-cyberattack-affecting-16000-patients.

[50] M. Field, "WannaCry cyber-attack cost the NHS £92m as 19,000 appointments cancelled," Technology Intelligence, visitado em 07-2023. URL: https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

[51] S. Ragupathy and M. Thirugnanam, "IoT in Healthcare: Breaching Security Issues Security Breaches and Threat Prevention on the Internet of Things," Adv. Inf. Secur. Privacy, Ethics (AISPE), B. Ser., no. February, 2017.

[52] R. Maria and O. Ribeiro, "Segurança em IoT: simulação de ataque em uma rede RPL utilizando Contiki," p. 70, 2018.

[53] L. S. Medeiros, P. E. Strauss, D. Sc, M. Sc, and M. Sc, "Segurança da informação para desenvolvimento e utilização de IoT," 2017.

[54] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of Security and Privacy Issues of IoT," pp. 1–7, 2012.

[55] ENISA, Good Practices for Security of Internet of Things in the context of Smart Manufacturing NOVEMBER 2018 Good practices for Security of Internet of Things in the context of Smart Manufacturing About ENISA, no. November. 2018.

[56] ENISA, Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, no. November. 2017.

[57] S. Krushang and H. Upadhyay, "A survey on Internet of Things," Int. J. Eng. Res. Dev., vol. 10, no. 11, pp. 58–63, 2014.

[58] Garcia-Morchon, "RFC 8576: Internet of Things (IoT) Security: State of the Art and Challenges," pp. 1–50, 2019.

[59] M. Digital, "Segurança em Redes de Computadores," pp. 1–8, 2013.

[60] S. Patients, D. Against, G. Threats, and B. Cybersecurity, "Securing the Internet of Healthcare Things The current threat landscape for the EoT The challenge for organizations," pp. 1–12, 2018.

[61] H. Journal, "89 Percent of Healthcare Organizations Have Experienced a Data Breach," HIPAA Journal, visitado em 05-2023. URL: https://www.hipaajournal.com/ponemon-89-pc-healthcare-organizations-experienced-data-breach-3430/.

[62] H. Journal, "87% of Healthcare Organizations Will Adopt Internet of Things Technology by 2019," HIPAA Journal, visitado em 05-2023. URL: https://www.hipaajournal.com/87pc-healthcare-organizations-adopt-internet-of-things-technology-2019-8712/.

[63] R. C. Keith A. Stouffer, "Measuring Impact of Cybersecurity on the Performance of Industrial Control Systems," NIST, 2014. visitado em 05-2023. URL: https://www.nist.gov/publications/measuring-impact-cybersecurity-performance-industrial-control-systems.

[64] M. Hogan and B. Piccarreta, "Interagency report on the status of international cybersecurity standardization for the internet of things (IoT)," 2018.

[65] OWASP, "OWASP Internet of Things Project." visitado em 06-2023. URL: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Medical_Devices.

[66] "OWASP Top 10 vulnerabilidades." visitado em 05-2023. URL: https://www.owasp.org/images/thumb/7/79/OWASP_2018.

[67] ASSEMBLEIA DA REPÚBLICA, "Lei n.o 46/2018 Regime jurídico da segurança do ciberespaço," pp. 4031–4037, 2018.

[68] Shirey, "RFC 2828: Internet Security Glossary This," Internet Secur. Gloss., vol. 9, no. 2, pp. 1–212, 2000.

[69] OWASP, "Top IoT Vulnerabilities," OWASP, 2016. visitado em 07-2023. URL: https://www.owasp.org/index.php/Top_IoT_Vulnerabilities.

[70] O. Digitasl, "A botnet Mirai está de volta e ameaça a internet. Saiba como se proteger!," 2019.

[71] G. Weidman, Penetration Testing - A hands on introduction to Hacking. 2014.

[72] CSO, "SQLi, XSS zero-days expose Belkin IoT devices, Android smartphones," visitado em 07-2023. URL: https://www.csoonline.com/article/3138935/sqli-xss-zero-days-expose-belkin-iot-devices-android-smartphones.html.

[73] W. N. Yard, "Manufacturer Usage Description Specification This - RFC8520," pp. 1–60, 2019.

[74] NIST, "NATIONAL VULNERABILITY DATABASE." visitado em 07-2023. URL: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

[75] D. Wood, N. Apthorpe, and N. Feamster, "Cleartext Data Transmissions in Consumer IoT Medical Devices," 2018.

[76] CISA, "Medtronic MiniMed 508 and Paradigm Series Insulin Pumps," 2019. [Online]. Available: https://www.us-cert.gov/ics/advisories/icsma-19-178-01

[77] HP, "The Insecurity of Network-Connected Printers: Executive Summary Sponsored by HP Independently conducted by Ponemon Institute LLC," no. September 2015.

[78] Internet Society, "IoT Security & Privacy Trust Framework v2.5," pp. 1–6, 2017.

[79] IoT Security Foundation, "IoT Security Compliance Framework," 2017.

[80] A. Mater and S. Universit, "Managing Challenges of Non-Communicable Diseases during Pregnancy: An Innovative Approach Tesi in Sistemi Distribuiti," 2017.

[81] A. Albataineh and I. Alsmadi, "IoT and the Risk of Internet Exposure: Risk Assessment Using Shodan Queries," pp. 1–5, 2019.

[82] E. McMahon, R. Williams, M. El, S. Samtani, M. Patton, and H. Chen, "Assessing medical device vulnerabilities on the Internet of Things," 2017 IEEE Int. Conf. Intell. Secur. Informatics Secur. Big Data, ISI 2017, pp. 176–178, 2017.

[83] D.-L. n.º 65/2021, Decreto-Lei n.º 65/2021, Documento, visitado em 09-2023. URL: https://dre.pt/dre/detalhe/decreto-lei/65-2021-168697988.