Gestão e Sensorização do Laboratório de Redes e Sistemas do ISMAI

Mestrado em Tecnologias da Informação, Comunicação e Multimédia

Ramo de Telecomunicações

Candidata: Maria João Abrantes Lage nº30415

Supervisor: Professora Cláudia Freitas

Maia, 29 de janeiro de 2021

Resumo

A recente transformação do Laboratório de Redes e Sistemas Informáticos do ISMAI permitiu uma melhor organização dos equipamentos e até a melhoria das condições em que estes se encontravam. Como consequência, o Laboratório 10 tornou-se numa sala capaz de suportar mais disciplinas, docentes e alunos. Verificou-se, também um aumento do interesse dos alunos pois, para além do aumento da variedade de equipamentos, as alterações efetuadas proporcionaram uma melhoria na qualidade do ensino.

No entanto, como em qualquer ampliação, também esta trouxe mais vulnerabilidades ao laboratório enquanto sala de aula, e à sala técnica, que recebeu um significativo aumento de equipamentos.

Outro desafio decorrente do aumento dos equipamentos disponíveis para as aulas é a complexidade acrescida no trabalho de preparação dos equipamentos para aulas práticas e testes. Nesse caso, este relatório propõe a criação de uma plataforma que permita uma gestão mais automatizada dos ficheiros de configuração dos equipamentos.

No mesmo contexto de vulnerabilidades mencionado acima, também se considerou importante a aplicação de um conjunto de sensores que permitisse uma melhor gestão das condições ambientais da sala técnica e do controlo de acessos à mesma.

Por fim, e com base nos motivos apresentados, foi feito um relatório de análise do risco que avalie as necessidades para o melhoramento da gestão do risco no laboratório 10, mesmo este não sendo uma organização por si só.

Abstract

The recent transformation of ISMAI's Network and Computer Systems Laboratory allowed for a better organization of the equipment and even the improvement of the state of such equipment. As a result of this improvement, Laboratory 10 became more appealing to other curricular units, teachers and students. It was even possible to conclude that the students began to become more motivated because it provided an enhancement in the quality of teaching.

Another challenge resulting from the increase in available devices is the increased complexity that applies to the task of provisioning them for the classes and assessments. This also exposed more vulnerabilities of the laboratory itself, as a classroom and technical room, which saw its equipment pool grow significantly.

With the increase of available equipment, the classes became more complex and preparation of said classes became especially tedious. This report proposes the creation of a platform that allows to manage equipment configuration files more dynamically.

Within the same context of vulnerabilities previously mentioned, it was deemed important to build and apply a set of sensors that would allow a better management of the environmental conditions of the technical room and its access control.

Finally, and based on the arguments presented above, a risk analysis report was produced in order to evaluate what is necessary and essential for the improvement of risk management in Laboratory 10, even though it is not an entity by itself.

Agradecimentos

Os meus primeiros agradecimentos vão para a minha orientadora, Professora Cláudia Freitas, pois foi uma professora muito presente, empenhada e sem ela não conseguiria atingir este objetivo. Também quero agradecer ao Professor João Paredes pela ajuda ao longo de todo o projeto.

Em segundo lugar quero agradecer aos meus pais, avós e tio, foram peças fundamentais para a minha estabilidade emocional e motivação. O mesmo posso dizer do meu namorado Bruno Martins, uma pessoa presente em todos os momentos deste projeto, apesar de toda a situação que se passou no último ano.

Aos meus melhores amigos, Bruno Ferreira e Nuno Santos, só tenho de agradecer por todo o esforço que fizeram para me ajudar. Ao Bruno Guimarães também devo um grande agradecimento, ele nunca hesitou em me ajudar e não há palavras que possam descrever o quanto agradeço por isso.

Por fim, quero deixar um agradecimento a todas as outras pessoas que participaram neste projeto de uma maneira ou de outra.

Um grande obrigado a todos!

Índice

Lista de Figuras

Lista de Acrónimos

AC - *Alternating Current*

ACK - *Acknowledgments*

ACL - *Access Control List*

ACL - *Asynchronous Connection-Less*

AES - *Advanced Encryption Standard*

AMI - *Advanced Metering Infrastructure*

AP – *Access Point*

BASH - *Bourne-Again Shell*

BLE - *Bluetooth Low Energy*

BSS - *Basic Service Set*

CCTV – *Closed-circuit Television*

CISO - *Chief Information Security Officer*

COO - *Chief Operating Officer*

CSMA-CA - *Carrier Sense Multiple Access-Collision Avoidance*

D2D - *Device to Device*

DC - *Direct Current*

DES - *Data Encryption Standard*

DPO - *Data Protection Officer*

DPO - *Data Protection Officer*

DS - *Distribution System*

DSSS - *Direct Sequence Spread Spectrum*

ESS - *Extended Service Set*

FFD - *Full Function Device*

FH/TDD - *Frequency Hopping / Time Division Duplex*

FHSS - *Frequency Hop Spread Spectrum*

FK - *Foreign Key*

GSM - *Global System for Mobile Communications*

GTS - *Guaranteed Time Slot*

HEMS – *Home Energy Management System*

IBM - *International Business Machines Corporation*

IBSS - *Independent Basic Service Set*

ICN - *Information-Centric Networking*

IEC - *International Electrotechnical Commission*

IoT – *Internet of Things*

IP – *Internet Protocol*

ISM - *Industrial, Scientific and Medical*

ISO – *The International Organization for Standardization*

ITU-R - *International Telecommunication Union - Radiocommunication Sector*

LAN - *Local Area Network*

LTE - *Long Term Evolution*

M2M - *Machine-to-Machine*

MAC – *Medium Access Control*

MANET - *Mobile Ad hoc Network*

MEMS - *Micro Electro-Mecanical Systems*

MIC - *Message Integrity Code*

M-MIMO - *Massive Multiple-Input Multiple Output*

MQTT - *Message Queuing Telemetry Transport*

NCM – *Network Configuration Manager*

NFC - *Near Field Communication*

NTP - *Network Time Protocol*

OID - *Object Identifiers*

OLTs – *Optical Line Terminal*

PAN - *Personal Area Network*

PHP – *Personal Home Page / Hypertext Preprocessor*

PWM – *Pulse Width Modulation*

QNRCS – Quadro Nacional de Referência para a Cibersegurança

QoS - *Quality of Service*

RBAC - *Role-base Access Control*

RFD - *Reduced Function Device*

RFID - *Radio-Frequency IDentification*

RSSF - Rede de Sensores sem Fios

SCO - *Synchronous Connection-Oriented*

SCP - *Secure Copy Protocol*

SGBD – Sistema de Gestão de Base de Dados

SMS - *Short Message Service*

SNMP - *Simple Network Management Protocol*

SPI – *Serial Peripheral Interface*

SQL - *Structured Query Language*

SSH - *Secure Socket Shell*

VPN - *Virtual Private Network*

WSN - *Wireless Sensor Network*

1 Introdução

Em 2019 foi criada, no ISMAI, uma nova sala técnica. Esta sala técnica foi criada para conseguir receber os novos equipamentos Cisco. Na nova sala técnica também terão lugar os elementos que já faziam parte da antiga sala técnica, equipamentos Nokia, OLTs e servidores. Este projeto tem como objetivo dotar a nova sala técnica de ferramentas e métodos para gerir, monitorizar e cuidar da nova sala técnica. Com o aumento do número de equipamentos, torna-se muito difícil que os docentes responsáveis pela sala técnica consigam gerir e cuidar de todos os equipamentos agora lá presentes.

O projeto será focado em três diferentes fases. A primeira fase passa pela idealização de uma plataforma que permitirá a gestão das configurações dos equipamentos presentes na sala técnica. Esta gestão das configurações permitirá que seja feito o *download* e *upload* das configurações dos equipamentos de forma mais automatizada, ao contrário do que acontece atualmente.

A segunda fase, que terá mais foco no laboratório como um todo, passará pela criação de um conjunto de sensores, interligados em rede, e que terão a função de monitorizar diversos pontos da sala e de controlar os acessos tanto ao laboratório como à sala técnica. De forma a serem analisados os dados recolhidos pelos sensores, serão criados painéis de controlo para que os resultados das leituras possam ser acompanhados de forma mais intuitiva. Por fim, serão criados alertas para que as pessoas responsáveis pelo laboratório possam receber os avisos de quando algo não está a funcionar corretamente.

A última fase deste projeto passará pela criação de um relatório de gestão do risco referente ao laboratório 10, em que o objetivo do mesmo é dar a entender quais as atividades necessárias serem postas em prática relativamente à gestão do risco no espaço em questão.

1.1 Contexto

A longo de todo o ano de 2019 foi criada, no ISMAI, uma nova sala técnica do laboratório de redes e sistemas informáticos. A sala tem como atual conceito a junção de diversos equipamentos presentes no anterior laboratório e de novos equipamentos Cisco.

A sala é constituída por diversos tipos de equipamentos: servidores, OLTs, *firewalls*, *routers* e *switches* Cisco e *routers* Nokia (antiga Alcatel Lucent Canadá), sendo este último resultado de um contrato estabelecido entre a atual Nokia, o Instituto Universitário da Maia e a Associação Porto Digital, a maio de 2011. Este protocolo foi estabelecido para a criação do primeiro Centro Ibérico de Formação Avançada e Certificação da Alcatel-Lucent em Telecomunicações na Área das Redes de Nova Geração. Como é percetível, esta nova sala técnica é constituída por diversificados tipos de equipamento e em maior escala, sendo de maior complexidade a sua gestão. Com o passar dos anos letivos, o número de alunos a ter aulas naquela sala tem vindo a aumentar consideravelmente por ser uma sala bastante importante para o ensino de diversas unidades curriculares. Consequentemente, o uso dos equipamentos por parte dos docentes e alunos aumenta, passando a ser uma ferramenta fundamental para o ensino/aprendizagem.

O primeiro grande objetivo é a idealização de uma plataforma que permita transferir configurações dos equipamentos de forma mais automatizada, ultrapassando o método atualmente utilizado e que tira algum tempo às aulas. Ainda relativamente à sala técnica e com a experiência de acontecimentos anteriores, pensou-se que seria essencial, para o bom funcionamento da sala, a criação de um conjunto de sensores que permita monitorizar todos os equipamentos e condições ambientais/energéticas com o objetivo de prevenir ou atuar de forma mais rápida e eficaz em situações de risco para os equipamentos. Também se considerou importante, e de forma a automatizar a entrada dos alunos no laboratório, a criação de controlos de acesso à sala técnica, sendo apenas permitida, fora do tempo de aulas, a entrada a alunos inscritos a unidades curriculares lecionadas naquela sala.

Por fim, com base em todas as razões já apresentadas, foi considerado importante a criação de um relatório de gestão do risco do laboratório 10. Este relatório permitirá a análise

da gestão do risco atualmente presente no laboratório 10 e de que forma poderá ser melhorada de forma a garantir uma maior segurança.

1.2 Motivação

Anteriormente à sala técnica que é discutida neste documento, existiu uma versão mais pequena que apenas era constituída por *routers* da Nokia e bastidores colocados nas mesas da sala, para que fosse de fácil acesso aos alunos. Os restantes equipamentos utilizados eram ligados de forma externa e conforme o essencial para as aulas práticas, testes práticos ou projetos. Nesta nova sala técnica, o objetivo foi, para além da inserção dos novos equipamentos, melhorar a organização dos equipamentos e reestruturar o espaço, permitindo a inserção de todos os equipamentos necessários para um ano letivo de aulas em qualquer grau de ensino. A sala sendo bastante maior que a anterior, permitiu criar melhores condições para que os docentes pudessem organizar melhor as suas aulas/testes práticos e projetos.

Com o aumento da sala, do número de equipamentos e do número de alunos e docentes, a taxa de utilização dos equipamentos tem tendência a aumentar e, portanto, o fluxo de trabalho também. Tendo os docentes e os alunos a vantagem de ter mais equipamentos para trabalhar, também aumenta a complexidade de realizar a transferência do trabalho que foi executado nos equipamentos. A plataforma idealizada vai permitir melhorar a forma de gestão das configurações por parte dos docentes, desperdiçando-se menos tempo de aula no *upload* no início da aula, e *download* no fim da aula.

Com base em todos os tópicos abordados no parágrafo anterior e em acontecimentos anteriores, detetou-se que uma das insuficiências da sala técnica é o facto de a mesma não ter qualquer tipo de controlo ambiental/energético. As necessidades passam pelo controlo de acessos da sala (havendo controlo de quem entra na sala nos períodos fora das aulas), a melhoria do consumo energético na sala técnica (através da instalação de sensores de movimento de forma a reduzir a utilização da luz nos diferentes compartimentos da sala técnica) e sensores de temperatura e humidade do ar (de forma a proteger os equipamentos).

Serão criados painéis de controlo para apresentar todos os dados recolhidos pelos sensores através da rede. A recolha de dados é bastante importante para que se possa enviar alertas quando algum parâmetro apresenta desvio dos valores considerados normais.

Por fim, e não menos importante, foi identificada a necessidade da elaboração de um relatório de gestão do risco para o laboratório 10. Este relatório permite identificar o que está atualmente definido/implementado e de que forma o laboratório poderá estar seguro aos diversos riscos que o rodeiam.

1.3 Objetivos

Ao analisar o estado atual da interação dos docentes e alunos com o laboratório, a sala técnica e o laboratório remoto, definiu-se três grandes objetivos:

- Idealização de uma plataforma que permita fazer transferência de configurações dos equipamentos de forma mais automatizada e definir as funcionalidades da mesma.
- Implementar um conjunto de sensores que permita monitorizar todos os equipamentos e condições ambientais/energéticas da zona técnica do laboratório 10;
- Elaboração de um relatório de gestão do risco do laboratório de redes e sistemas informáticos do ISMAI.

De forma mais específica, e relativamente ao primeiro tópico, será idealizada uma plataforma que permitirá aos docentes transferir os ficheiros de configuração dos equipamentos presentes na sala técnica. A automatização deste processo tem como objetivo facilitar o processo aos docentes quando estes fazem algum tipo de atividade laboratorial, poupando o tempo de aula que é sempre dispensado para essas ações.

No que diz respeito aos sensores, pretende-se dotar o laboratório e sala técnica de diversos sensores, tais como temperatura, luz, humidade do ar, movimento com controlo de luzes, nível da água e corrente. Será também implementado um sistema de controlo de

acessos tanto no laboratório como na sala técnica. Os dados recolhidos pelos diversos sensores serão mostrados em painéis de controlo da plataforma para que possam ser analisados em tempo real. Pretende-se ainda que, caso se detete desvios anormais dos parâmetros em análise, sejam emitidos alertas de forma a avisar os responsáveis de alguma situação anómala, podendo, assim, proceder-se à resolução das falhas.

Por fim, a elaboração de um relatório de gestão do risco do laboratório de redes e sistemas informáticos do ISMAI. Este relatório permitirá entender quais são as necessidades do laboratório 10 no que diz respeito à gestão do risco do mesmo. Para a elaboração deste relatório foi feita uma prévia recolha de dados relativos ao laboratório 10 de forma a perceber o que é necessário melhorar.

1.4 Organização

O capítulo 1 é constituído pela Introdução e onde são mencionados o contexto, a motivação e os objetivos. O capítulo 2 é relativo ao estado de arte e trabalhos relacionados, desde o modelo FCAPS, a *software* de gestão da rede e *SmartRoom*. O capítulo 3 é relativo ao cronograma, sendo constituído pela lista de tarefas e o gráfico de Gantt. O capítulo 4 é referente à implementação de todos os objetivos definidos no capítulo 1. O capítulo 5 é a análise de resultados dos dados obtidos no capítulo anterior. O capítulo 6 são as conclusões finais do projeto. O capítulo 7 é relativo ao trabalho futuro possível de ser implementado com base neste projeto. O capítulo 8 são as referências utilizadas ao longo de todo o trabalho. E, por fim, o capítulo 9 são os anexos necessários a completar a informação colada no capítulo da implementação.

2 Estado de Arte e Trabalho Relacionado

As configurações são resultado dos diversos comandos executados e guardados em ficheiros específicos em cada equipamento. A gravação destes ficheiros tem ainda mais importância a nível laboratorial. Tanto os alunos como os docentes, atualmente, têm de fazer a transferência da configuração que criaram e que necessitam de utilizar. O objetivo da gravação destes ficheiros é que os docentes e os alunos tenham, de forma mais automática, acesso a esses ficheiros de cada um dos equipamentos presentes na sala técnica. Isto tem vantagens tanto em momentos de avaliação prática como em atividades laboratoriais porque reduz desperdícios de tempo com preparação.

2.1 Modelo FCAPS

O modelo *FCAPS* é uma *framework* que é utilizada no âmbito da gestão e monitorização de redes. A mesma foi criada pela ITU - *Telecommunication Sector* (ITU-T) e pela *International Organization for Standardization* (ISO) e é constituída por cinco áreas, que podem, ou não, fazer parte de um sistema de gestão. As cinco áreas são:

- Gestão de Falhas (*Fault*);
- Gestão de Configuração (*Configuration*);
- Gestão de Contas (*Accounting*);
- Gestão de Desempenho (*Performance*);
- Gestão de Segurança (*Security*).

2.1.1 Gestão de Falhas

A gestão de falhas tem como principal objetivo manter uma rede estável e funcional. A gestão de falhas é caracterizada pelo funcionamento coerente e contínuo, começando pela deteção, isolamento e correção dessas mesmas falhas. Segundo (Pires, 2018), as falhas podem ser eventos persistentes ou temporários. Os eventos temporários são também

importantes e devem ser devidamente registados, mas não necessitam de qualquer tipo de correção. No caso das falhas persistentes, estes podem precisar de atuação direta do administrador da infraestrutura e as mesmas devem ser reportadas através do uso de um sistema de alertas. É também importante que, independentemente da falha e/ou da correção (ou não) dada a uma determinada falha, a mesma fique registada de forma a ser possível prevenir ou prever futuras ocorrências.

2.1.2 Gestão de Configuração

A gestão de configuração, o segundo nível do modelo *FCAPS*, tem como principal objetivo a monitorização da configuração dos equipamentos da rede. Esta monitorização permite também que se possa fazer alterações nas configurações da rede e dos equipamentos, bem como a inserção de novos equipamentos na rede de gestão.

Uma tarefa também importante deste nível é o *backup* e restauro da rede. No caso de algum de ocorrer algum evento catastrófico que destrua ou corrompa as configurações de um equipamento, é humanamente impossível a sua reconfiguração manual em tempo útil, sendo obrigatório automatizar para recuperar a disponibilidade o mais rapidamente possível.

2.1.3 Gestão de Contas

O *accounting* tem a função de controlar e registar a utilização dos recursos/serviços da rede por parte dos utilizadores e clientes. O resultado de "*quantificar, medir, reportar, analisar e controlar o desempenho dos dispositivos da rede.*" (Marques, 2015) permite conhecer os hábitos de consumo dos utilizadores e, no caso de os recursos serem mais escassos, podem ser aplicadas medidas para definir limites de utilização ou otimizar a sua disponibilização.

2.1.4 Gestão de Desempenho

Na gestão de desempenho são definidas tarefas para a recolha e análise dos dados estatísticos da rede (Gil, 2012) e, se necessário, melhorar os níveis de desempenho da rede de modo a garantir a boa capacidade de tráfego para não comprometer quaisquer recursos necessários aos utilizadores da rede.

2.1.5 Gestão de Segurança

No último nível do modelo de gestão FCAPS, a gestão da segurança contempla políticas e regras que garantam o bom funcionamento e a boa utilização da rede, tendo medidas que previnam a entrada de utilizadores não desejados, criação de grupos e respetivos privilégios. Para além do mencionado anteriormente, a gestão da segurança é responsável também pela integridade e confidencialidade dos utilizadores e da sua informação.

2.2 Software de Gestão da Rede e de Configurações

2.2.1 SolarWinds

A SolarWinds é uma empresa americana que tem como foco de negócio a criação e desenvolvimento de *software* para a gestão de redes e sistemas de tecnologias de informação. A empresa desenvolveu produtos para seis áreas diferentes: gestão de redes, gestão de sistemas, segurança das tecnologias de informação, gestão de base de dados, central de ajuda e suporte remoto e, por fim, monitorização de aplicativos na nuvem (SolarWinds).

A nível de gestão da rede, são oferecidos diversos recursos que podem ser usados para estabelecer uma visão geral da rede e dos recursos. Esses recursos vão desde a verificação da conformidade da rede, à avaliação e correção de vulnerabilidades, gestão do

ciclo de vida dos equipamentos e controlo de todas as sessões e dispositivos com acesso autorizado ou não e quais as suas permissões.

A nível de segurança, a SolarWinds oferece a *Network Insight*, *frameworks* dedicadas a quem usa *Palo Alto Networks* ou *Cisco ASA* e a *Cisco Nexus* (*switchs*).

Mais focada na gestão das configurações, aos utilizadores é disponibilizada a opção de fazer *backup* das mesmas, permitindo a sua correção no caso de algo ter sido configurado incorretamente. Toda esta gestão e permanência da conformidade da rede é melhorada através do uso do *SolarWinds Network Performance Monitoring*.

2.2.2 ManageEngine - Network Configuration Manager

A *ManageEngine* resultou da divisão do fabricante indiano *Zoho Corporation*. Este fabricante de *software* oferece diversos produtos relacionados com a gestão das Tecnologias de Informação e como tem uma vasta lista de dispositivos em que pode ser instalado e utilizado tirando o maior proveito possível, torna-o num dos "*líderes do mercado em software para a monitorização de infraestruturas*" (IREO - Distribuidor de Soluções TI, 2019).

Entre muitos outros, o *Network Configuration Manager* é o produto que gere as configurações dos diversos dispositivos de uma rede.

Esta gestão começa pela automatização das cópias de segurança das configurações. A mesma é feita com base em *syslog messages*, isto é, sempre que um utilizador faz *log out* de um dispositivo, é comparada a configuração atual do dispositivo com a já anteriormente guardada no NCM (*Network Configuration Manager*). Com frequência, são feitos inícios e fins de sessão nos dispositivos de uma rede e isso vai resultar em que o *software* esteja sempre a executar *triggers Syslog*, sobrecarregando o servidor e, consequentemente, afetando o desempenho de todo o processo e dispositivos. Este processo pode ser personalizado, isto é, podem ser definidos e bloqueados os dispositivos que os administradores da rede decidam que não precisam de um controlo tão rigoroso.

Segundo ManageEngine NCM, as configurações de um dispositivo devem ser guardadas com frequência de forma a manter um repositório de configurações pronto para

ser restaurado em caso de emergência e, por isso, existe uma ferramenta que permite a definição de um intervalo de tempo individual, para a execução desses *backups*. Podem, também, ser definidos alertas no caso de falha da execução desses *backups* ou até em alterações de configurações. Sempre que uma configuração é guardada, é-lhe atribuído um número de versão, de forma crescente, para que os utilizadores consigam identificar qual a última versão implementada no equipamento.

Por fim, o NCM permite que possa ser definida, por equipamento, a chamada *Baseline Configuration*. Esta configuração é atribuída pelo utilizador da plataforma e o seu objetivo é que, sempre que alguma configuração com erros seja carregada, a *Baseline Configuration* seja carregada automaticamente pelo NCM para o equipamento, garantindo que o mesmo esteja com a configuração que permite o seu melhor desempenho.

2.3 Redes de Sensores e *SmartRoom*

A criação da Internet foi um passo tecnológico extremamente importante para o mundo. A comunicação entre as pessoas e a forma como as mesmas interagem com dispositivos com o objetivo de satisfazer vontades exigiu que a internet e a tecnologia tivessem uma evolução mais rápida nos últimos anos. O mundo tecnológico e da Internet cresceu rapidamente e de forma capaz de satisfazer diversas necessidades do Homem. Mais recentemente, o conceito de IoT (*Internet of Things*) ganhou muita força. A Internet das Coisas consiste, segundo Zheng, Simplot-ryl, Bisdikian, & Mouftah (2011), numa intercomunicação inteligente entre diversos objetos no mundo físico, tais como telemóveis, veículos, pessoas e das mesmas aos próprios objetos.

2.3.1 RSSF – Rede de Sensores sem Fios

A rede de sensores que mais tem crescido nos últimos tempos é a RSSF (Rede de Sensores sem Fios). Com o avanço dos chamados MEMS (*Micro Electro-Mecanical Systems*), microssistemas eletromecânicos, bem como novos métodos e dispositivos de

sensorização e microprocessadores, têm incentivado que sejam cada vez mais usados os sensores inteligentes em diversas áreas constituintes do nosso dia-a-dia.

A RSSF é um "*conjunto de dispositivos ou nós de sensores que, apesar de poderem funcionar de forma isolada e autónoma, têm capacidade para se agruparem e formarem redes de elevada dimensão, com o objetivo de monitorizar um conjunto de fenómenos físicos.*" (Sá Silva et al., 2016).

A *WSN* (*Wireless Sensor Network*) é um conceito diretamente associado às RSSF e tem como objetivo representar um conjunto de sensores/nós que comunicam entre si. A evolução, nos últimos anos, de protocolos como os IEEE 802.15.4 e o *ZigBee*, moveu a tecnologia dos laboratórios de testes e pesquisas para o uso em todo o tipo de áreas no dia-a-dia, tais como medicina, monitorização ambiental, deteção de intrusos, entre outros. (Teixeira De Gouveia, 2009) (Wheeler, 2007)

Como mostra a figura 1, nas *WSN*, existem nós coordenadores que recebem dados de diversos nós sensores e guardam os dados lidos por cada sensor. O número de nós coordenadores vai depender da topologia e de quantos nós sensores e que tipos de dados estes recolhem e em que quantidade.

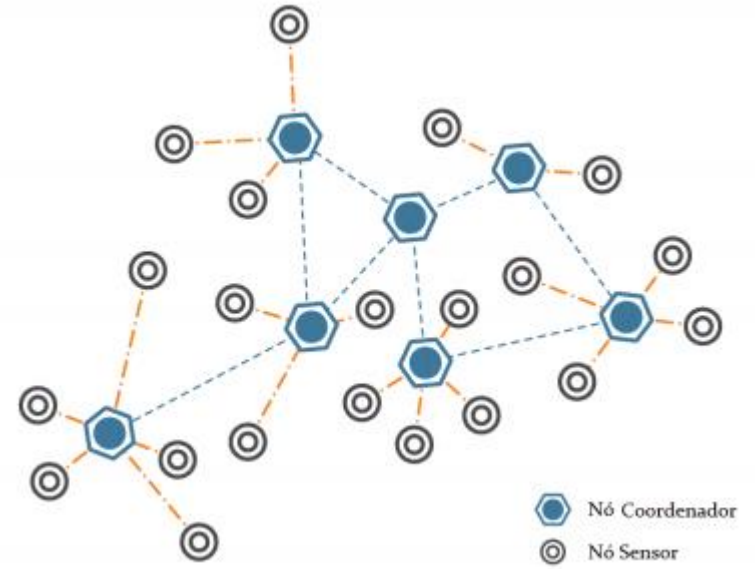


Figura 1 – *Wireless Sensor Network* (Mota, 2013)

2.3.2 Arquitetura geral de uma Rede de Sensores

O funcionamento de redes de sensores sem fios é com base em MANET (*Mobile Ad hoc Network*). Este funcionamento é conhecido por permitir que exista um número elevado e distribuído de nós e que os dados recolhidos por cada um desses nós possa ser passado pelos elementos constituintes dessa rede, até chegar à Internet. Os nós, idealmente, devem possuir mecanismos para uma gestão automatizada (manutenção, configuração, proteção, etc) (Beatrys Ruiz et al., 2004) (Ruiz, 2003).

Com uma arquitetura mais básica, (Glória et al., 2017), criaram um pequeno exemplo de uma rede de sensores para ambientes em geral. A arquitetura foi pensada de forma a que se pudesse adaptar facilmente aos requisitos do utilizador e que permitisse o uso de todos os protocolos de comunicação e de recolha de dados sensoriais, sendo estes feitos por *Ethernet* ou *wireless*.

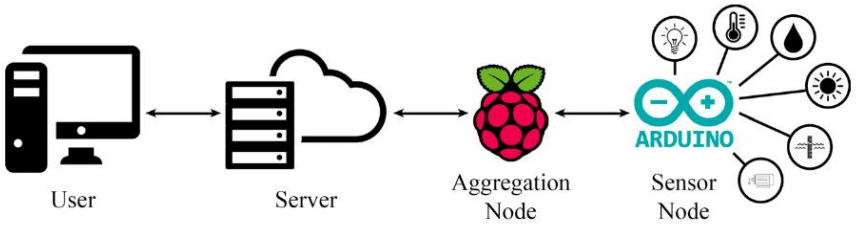


Figura 2 – Arquitetura do Sistema (Glória et al., 2017)

Com base na figura 2, apresentada pelos autores do documento, o *sensor node* é usado para recolha da informação de cada sensor e gestão de utilizadores. Neste caso em específico, o nó de agregação é usado como *gateway* entre o utilizador e os nós de sensores e procede a uma pequena análise dos dados recolhidos.

Nesta arquitetura, a nível de *software*, é feita uma conexão entre o utilizador e a rede de sensores usando *Eclipse Paho JavaScript Client*, que tem como base o protocolo MQTT (*Message Queuing Telemetry Transport*). Os dados recolhidos pelos sensores chegam ao protocolo *MQTT* através de um *script* em *Python*.

O *MQTT*, baseado em TCP/IP, foi criado em 1999 pelo Dr. Andy Stanford-Clark da IBM (*International Business Machines Corporation*) e Arlen Nipper da Arcom (atual *Eurotech*), sendo, atualmente um protocolo standard da IEC (*International Electrotechnical Commission*) (IEC, 2016).

Segundo Thomas & Kumar, 2019, este protocolo serve para conectar dispositivos instalados em locais remotos. A comunicação base deste protocolo é M2M (*Machine-to-Machine*) e foi criado para ser suportado por dispositivos mais pequenos, com menos capacidade de *hardware* e largura de banda mais estreita. O *broker* tem como função receber os dados enviados pelo *middleware broker* associado ao MQTT é usado para fazer a troca de mensagem entre os *publishers* e os *subscribers*, sendo que a troca de mensagem é feita no método *publish*/*subscribe*.

O MQTT, no trabalho anteriormente analisado, tem como função recolher os *scripts* presentes no nó de agregação e interligá-los com a plataforma *web*. Os *scripts* são um componente fundamental pois são eles os responsáveis pela circulação dos dados recolhidos pelos sensores. O *script*, com base num tempo previamente definido, indica ao sensor que

tem de recolher dados e prepara a entrada na base de dados onde serão armazenados esses dados. A plataforma *web* tem como principal objetivo mostrar os dados inseridos na base de dados de forma mais intuitiva e simples de analisar.

Um ponto a ter em consideração é se é ou não possível que, em arquiteturas mais completas e complexas, sejam conjugados diferentes *nodes*, *gateways* e tecnologias de comunicação.

Segundo Mukherjee & Biswas, 2018, os nós de sensores podem captar diferentes parâmetros no mesmo ambiente, guardar os dados recolhidos de forma temporária e comunicar com outros dispositivos através de diversas tecnologias já existentes e não tão complexas.

A arquitetura deste trabalho foi construída pelos autores com base em hierarquias, isto é, a rede de comunicação é divida em quatro hierarquias

- *"H-1: Wireless Sensor Network (WSN).*
- *H-2: Mobile Adhoc Network (MANET).*
- *H-3: WLAN and/or Internet gateway.*
- *H-4: Internet."* (Mukherjee & Biswas, 2018).

Esta hierarquia começa nos nós de sensores, que estão interligados em grupos por *gateways*. As informações recolhidas pelos sensores são enviadas por estas *gateways* para os dispositivos presentes na H-2 e H-3. Os nós MANET recolhem os dados que estão nas *gateways* e transmitem-nos em direção à Internet (H-3). Neste nível, foi considerada uma estrutura WLAN que teria equipamento que estaria diretamente ligado, por cabo, à Internet (H-4), de forma a aumentar e assegurar a entrega dos dados.

Para os autores, a arquitetura de rede hierárquica traz vantagens no sentido em que o nível 1 pode comunicar diretamente com o nível 2 ou o nível 3, dependendo da prioridade/importância do tráfego.

Mukherjee & Biswas (2018) explicam que uma arquitetura por hierarquias/níveis tem diversas vantagens comparativamente ao modelo convencional de dois níveis (mistura de elementos da rede que consomem pouca energia com os que consomem muita). A junção de

nós MANET à arquitetura uniformiza as diferenças entre os diferentes dispositivos da rede, conseguindo otimizar diversas características da rede, tais como:

- Atraso da transmissão de pacotes, pois os nós MANET são geridos por um algoritmo (proposto pelos autores) que permite a escolha do caminho mais pequeno desde o nó até à Internet;
- Escalabilidade, no sentido em que nós MANET conseguem interligar-se a nós de sensores que diferem nas tecnologias utilizadas e coletar os dados de todos;
- A energia utilizada por cada nó da rede é eficientemente distribuída de forma a que todos contribuam para a passagem dos pacotes de dados até à Internet uniformemente.

Os autores criaram duas aplicações IoT com a arquitetura mencionada nos parágrafos anteriores. Para entendermos melhor que é possível a interligação de diversas tecnologias na mesma arquitetura, é importante percebermos o que foi usado em cada aplicação a nível da *stack* protocolar.

A primeira aplicação é um "*Hospital information System (HIS)*" (Mukherjee & Biswas, 2018). É dada a cada doente uma pulseira com sensores para fazer a medição padrão do estado do doente (pressão arterial, temperatura, etc). O administrador tem a função de configurar para aquela pulseira todas as informações de interesse para gestão interna, o *ID* do médico, as doenças associadas ao paciente numa fase de admissão, e o *ID* da cama em que será colocado o doente, entre outros dados. Para além disso, os prestadores de cuidados e suporte também usarão um dispositivo e as camas terão um sensor de deteção de ocupação. Todos estes sensores permitirão recolher os dados para uma melhor gestão do espaço hospitalar (ocupação de camas, número de doentes tratados por dia, disponibilidade dos prestadores, etc).

As pulseiras dos doentes, na camada de *link*, terão a tecnologia IEEE802.15.4 (IEEE, 2019), por ter consumos energéticos muito reduzidos, aumentando o tempo de vida da bateria do dispositivo. Na camada de rede, usa IPv6. O protocolo 6LowPan (Shelby & Bormann, 2011), que foi criado para ser usado em dispositivos que usem IEEE802.15.4 (Kim et al., 2012), permite que sejam interligadas as camadas de MAC e de *routing*. Como demonstrado

na Figura 3, o *routing* não é exatamente igual ao do IP, isto é, este apenas faz a interligação entre as camadas e permite que seja feita, na mesma, a fragmentação e a reassemblagem necessária para a correta formação dos cabeçalhos do pacote. A interligação entre este protocolo e esta tecnologia leva a ser necessário ter cuidado com diversos possíveis problemas, sendo um deles o tamanho dos pacotes não corresponder ao tamanho da *frame* usada no IEEE802.15.4.

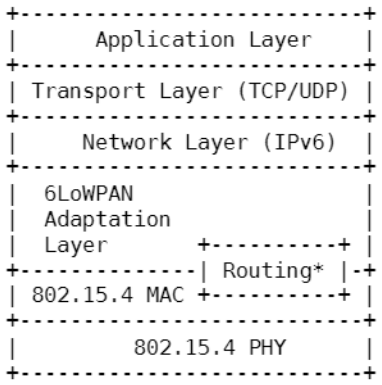


Figura 3 – Representação do *routing* de 6LowPan numa *stack* de rede (Kim et al., 2012)

Após este processo, o pacote segue em direção à Internet através de *gateways*. Na topologia base deste estudo, as *gateways* têm comunicação direta com dois componentes da topologia: os sensores dados aos doentes e com os nós MANET. A comunicação tem por base pilhas protocolares de funcionamento distinto. A IEEE802.15.4 é usada para a conexão com os dispositivos sensoriais dados aos doentes, e o IEEE802.11, específico para *Wi-Fi* (H. Mahmoud, 2007), é usado para a conexão com os nós MANET, todos na camada de ligação.

A correta comunicação destes componentes é extremamente importante para o funcionamento de toda a rede, evitando assim a perda de pacotes. Assim sendo, é importante a distinção dos canais de frequência em que a comunicação será feita, sendo que a técnica usada para a deteção de colisões foi a CSMA-CA.

A segunda aplicação passa por uma pulseira para monitorizar jogadores de futebol. Esta pulseira é usada para a leitura de diversas características físicas e moleculares do

jogador. A comunicação entre estes dispositivos e o dos árbitros é feita por BLE (Bluetooth Low Energy). Os dispositivos usados pelos árbitros funcionam com ambas as tecnologias, BLE e IEEE802.11, pois funcionam como *gateway*. Os dados recolhidos pelos árbitros são enviados para um nó MANET que circula no campo (IEEE802.11), que por sua vez enviam para um nó MANET que está fixo, na rua, e através deste a informação segue para a *gateway* da Internet.

Ambas as tecnologias trabalham em 2,4GHz da banda ISM (*Industrial, Scientific and Medical*), com uma largura de banda de 83.5 MHz. Os autores entenderam que as comunicações, ao serem feitas na mesma banda, irão causar interferências entre os dados transmitidos por ambas as tecnologias, havendo uma alta taxa de probabilidade de perda de informação. Por isso, definiram que ambas as tecnologias irão ter formas de passagem de informação distintas, isto é, o IEEE802.11 irá funcionar com base em DSSS (*Direct Sequence Spread Spectrum*) (*DSSS - Direct Sequence Spread Spectrum - YouTube*, n.d.) e a BLE com base em FHSS (*Frequency Hop Spread Spectrum*) (*FHSS - Frequency Hopping Spread Spectrum - YouTube*, n.d.). DSSS, com o uso propositado de ruído, pega no pacote dos dados/informação, transmite de forma encriptada cada *bit* do respetivo pacote e a frequência será muito maior. FHSS, tal como o próprio nome indica, faz saltos entre diversas frequências ao longo de todo o envio/receção. Tradicionalmente, os pacotes são todos enviados pelo mesmo canal, sendo mais propício a ataques e interferências. O que esta tecnologia fará é, entre todos os canais definidos no espectro que varia entre 2.4GHz e 2.4835GHz, periodicamente vai mudar o canal em que a transmissão é efetuada.

Em suma, os autores conseguiram, com arquiteturas extremamente distintas, provar que diferentes tecnologias podem ser usadas no mesmo ambiente IoT. Na primeira aplicação, eles conseguiram fazer uma ligação entre duas camadas extremamente importantes em IoT, com recurso ao protocolo 6LowPan. Na segunda aplicação, foram interligadas tecnologias num só dispositivo (árbitro), sendo que este funciona como *gateway*. Os jogadores usam uma pulseira que comunica através de BLE com os dispositivos mencionados anteriormente. Para o dispositivo enviar os dados para a Internet usa o protocolo IEEE802.11.

2.3.3 Descoberta e automatização dos dispositivos

O conceito de Internet das Coisas não é recente e, por isso, são diversas as suas definições. Pode ser definida como a junção de protocolos eficientes e servidores *web* (Ashraf et al., 2016) que, com o uso de IP, conseguem conectar sensores presentes em casa, estações de meteorologia e outros elementos pertencentes ao nosso dia-a-dia. (Shelby & Bormann, 2011).

As redes IoT têm como característica o facto de se juntarem à rede, todos os dias, inúmeros dispositivos que se conectam à Internet. Com o aumento do número de dispositivos IoT, é importante ter-se em conta vários aspetos, tais como a escalabilidade e a gestão dos dispositivos. Segundo Ashraf, Habaebi, Islam, & Khan, 2016, a escalabilidade em IoT é caracterizada pela capacidade de conciliar o nível de desempenho elevado, consequente do aumento do número de dispositivos, com o aumento do fluxo de comunicação e de dados. Estes problemas são frequentes em WSNs (*Wireless Sensor Networks*).

A gestão manual dos dispositivos é uma função cada vez mais complexa e, por isso, a automatização da gestão dos dipositivos é cada vez mais tida em conta no que toca a redes IoT, principalmente nos dispositivos finais/terminais/sensores.

A gestão autónoma dos dispositivos "nasceu" com a IBM, em 2003, com a criação de uma *framework* que permitisse o controlo, em *loop*, dos dispositivos naquela rede. De forma a perceber melhor este conceito, podemos observar a Figura 4.

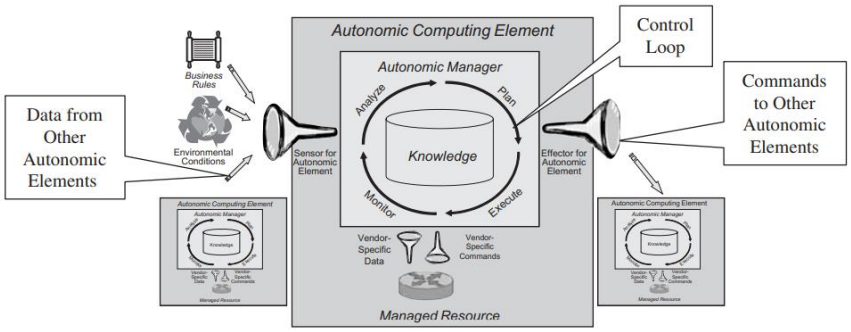


Figura 4 – IBM's autonomic control loop (H. Mahmoud, 2007)

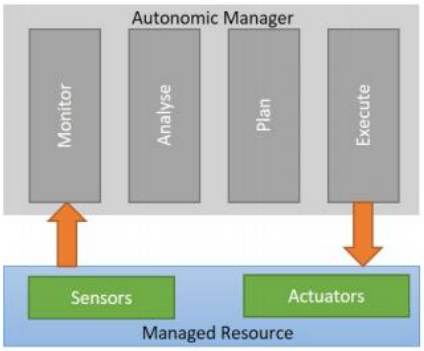


Figura 5 - IBM's autonomic control loop adaptado ao ambiente IoT (Chess & Kephart, 2003; Tahir et al., 2019)

Como se pode verificar nas Figuras 4 e 5, a *framework* tem dois componentes: *Managed Resource* e *Autonomic Manager*. Cada um destes componentes tem funções distintas, mas essenciais no que toca à automação dos sistemas. Segundo Chess & Kephart, 2003 e Tahir et al., 2019, a *Managed Resource* é constituída por todos os objetos/dispositivos (Figura 5) que possam recolher os dados do ambiente em que os dispositivos se integram e guardar esses mesmos dados temporariamente. Na mesma figura, podemos verificar a existência de atuadores, que têm a função de executar os pedidos feitos pelo *Autonomic Manager* de forma a alterar algum estado do sistema, do ambiente ou de um objeto.

O *Autonomic Manager*, segundo H. Mahmoud, 2007 e a Figura 4, usa um ciclo de controlo para monitorizar o estado de um determinado objeto (*Managed Resource*) e procede à sua correção no caso de o mesmo não estar operacional. O *control loop* é constituído por quatro módulos de funcionamento (Ashraf et al., 2016):

- Monitorizar – módulo responsável por recolher os dados referentes a um objeto em específico. Esses dados são agregados, filtrados e processados de forma a serem utilizados pelo módulo seguinte;
- Analisar – cria mecanismos que permitam o conhecimento, por parte do gestor autónomo, do ambiente em que estão inseridos os objetos e prevenir possíveis situações;

- Planear – com a definição de políticas, permite que se possa criar mecanismos para atingir determinados objetivos;
- Executar – executa os mecanismos previamente estabelecidos pelo módulo anterior e interage com os objetos, simultaneamente.

Em suma, ambas as entidades estão interligadas entre si e, no caso de algo falhar, é necessário que todos os módulos trabalhem de forma correta para que o problema se possa resolver, ou, até mesmo, prever.

Segundo Tahir et al., 2019, o paradigma na gestão autónoma das redes IoT, apesar de ter como base o que é apresentado por Chess & Kephart, 2003, terá que ter em conta diferentes sistemas, tais como: *self-configuration*, *self-optimization*, *self-healing*, *self-protection*, *self-security*, *self-adaptation* e *self-organization*.

2.3.4 Standards de comunicação de dados e protocolos

2.3.4.1 Bluetooth

O *Bluetooth* é uma tecnologia de comunicação sem fios criada para permitir a conexão e comunicação de dispositivos eletrónicos portáteis numa curta distância. Geralmente, esta tecnologia é usada em redes *ad hoc*, isto é, em redes que todos os dispositivos estão interligados entre si, sem haver uma ligação para o exterior. (Haartsen, 1998)

Esta tecnologia permite a transmissão de dados através do uso de radiofrequência, utiliza uma banda ISM (2.45GHz), sendo que é dividida de 2.400 MHz a 2483.5MHz para a Europa e Estados Unidos da América e 2.471 a 2.497MHz para o Japão. A banda ISM é aberta a toda a gente, o que facilitou a adaptação da tecnologia aos dispositivos já existentes, mas tem a desvantagem de ser suscetível a mais interferências externas (fornos micro-ondas são os que mais provocam interferência). Para combater este problema, o *Bluetooth* utilizou o método *frequency-hopping spread spectrum* (FHSS). Esta forma de comunicação faz com

que a frequência seja dividida em vários canais, tal como foi anteriormente mencionado na secção 2.3.2, referente ao BLE.

Esses canais usam o método FH/TDD (*Frequency Hopping / Time Division Duplex*). Este método cria *slots* que são divididos em períodos de 625 microssegundos e cada pacote é transmitido em cada salto, logo em 1 segundo são feitos 1600 saltos. Estes tempos são controlados pelo *master* da rede de objetos (*piconet*), através do seu relógio.

O pacote que é transmitido tem um formato fixo, como mostra na Figura 6.

Figura 6 – Formato do pacote transmitido por Bluetooth (Haartsen, 1998)

O campo *Access Code* é transmitido pelo *master*, é único por canal e permite que os *slaves* consigam distinguir a origem do pacote. O campo *Header* é constituído por todas as informações necessárias para a identificação do dispositivo, tipo do pacote e controladores de erro do cabeçalho e do pacote, como um todo.

A comunicação entre os dispositivos é feita com base em dois padrões: SCO (*Synchronous Connection-Oriented*) e ACL (*Asynchronous Connection-Less*).

O primeiro padrão é caracterizado por aceitar uma comunicação simétrica e ponto-a-ponto, isto é, são fixados dois *slots* consecutivos para envio e receção. Este padrão é geralmente usado para transmissão de voz. No caso de ser perdido algum pacote, este será totalmente perdido e aquilo que chega ao objeto de destino é som com ruído.

O segundo padrão aceita comunicações simétricas e assimétricas e comunicações ponto-multiponto, isto é, todos os *links* são geridos e tidos em conta por esta comunicação. Este padrão permite que os pacotes que sejam perdidos possam ser reenviados, garantindo, assim, a integridade das comunicações e sendo ideal para a transmissão de pacotes de dados.

O BLE foi criado juntamente com a versão 4.0 do Bluetooth. Na secção 2.3.2 foi explicado que o BLE foi criado para ser usado em dispositivos/objetos inteligentes com uma capacidade e durabilidade baixa de bateria, isto é, foi criado com o intuito de poder economizar energia, logo, as baterias duram mais tempo. As técnicas usadas pela tecnologia para a redução do consumo de energia passam pela redução do volume de dados transmitidos e pela redução do alcance da comunicação. Apesar de esta tecnologia permitir alcances de até 30 metros, quanto mais curta a distância entre os dispositivos, maior a economia de energia.

2.3.4.2 ZigBee

ZigBee é uma tecnologia que foi apresentada a julho de 2005 e veio resolver o problema de não existir nenhuma solução que permitisse cumprir requisitos como baixo consumo de energia e a necessidade de uma boa fiabilidade da rede, não tendo como principal foco a necessidade de altas taxas de transmissão. (Saleiro & Ey, 2009)

Segundo Kinney, 2003, esta tecnologia tem como características o baixo consumo, fazendo com que as baterias dos dispositivos/objetos possam durar de meses a anos, permite um número significativo de dispositivos por rede (tal é permitido pelas camadas física e de MAC do IEEE 802.15.4). Devido à sua simplicidade no que toca à implementação e manutenção, é um protocolo que pode ser usado globalmente e usa a banda 2.4GHz.

Os tipos de tráfego que podem ser usados pela camada MAC do protocolo IEEE802.15.4 em *ZigBee* têm três modos possíveis: o modo periódico (em que é enviado um sinal – *beacon* - para o sensor para "acordá-lo", verifica-se a existência de mensagens, em caso negativo, o sensor volta a "adormecer", permitindo, assim, uma poupança da energia consumida por cada sensor na rede); o modo intermitente (permite o uso do modo anteriormente apresentado ou o sensor pode comunicar ele quando for necessário). Para além destes dois modos, as aplicações que necessitem de baixa latência, podem usar o método GTS (*Guaranteed Time Slot*) que, com o uso de QoS (Quality of Service), garante que cada

dispositivo/objeto/sensor tenha um intervalo de tempo fixo para a transmissão de tudo o que necessitar.

Com a junção das camadas física e MAC ao *ZigBee*, foram definidos dois tipos de dispositivos que podem estar presentes na rede. Os dois tipos de dispositivos são: FFD (Full Function Device) que é conhecido como o coordenador da rede, funciona em qualquer topologia e pode comunicar com qualquer dispositivo, independentemente da sua classificação; e o RFD (Reduced Function Device) que é limitado à topologia de estrela, que será explicada a seguir, nunca pode ser eleito coordenador da rede e apenas comunica com o coordenador da rede, não com outros RFD.

Nas Figuras 7 e 8, são mostradas as diferentes topologias que podem ser assumidas por estes dispositivos.

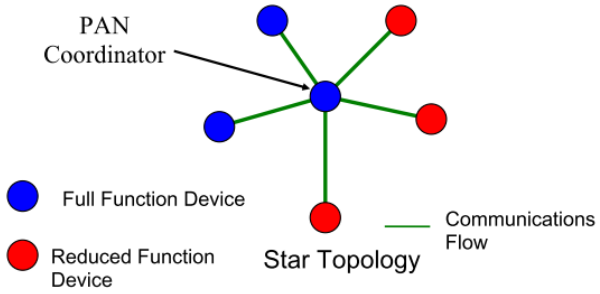


Figura 7 – Topologia em Estrela de uma PAN (*Personal Area Network*) (Patrick Kinney, 2003)

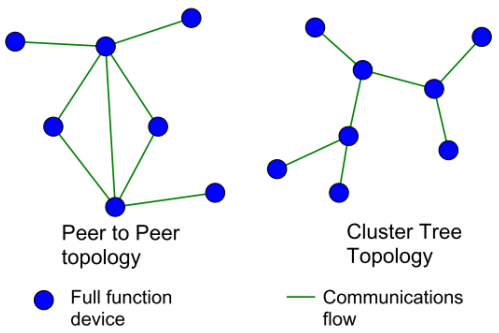


Figura 8 – Topologia Peer-to-Peer e Cluster de uma PAN (Patrick Kinney, 2003)

Para que possam ser corretamente construídas e geridas PANs, a IEEE802.15.4 MAC define quatro tipos de *frames*: *beacon*, usado pelo coordenador para a transmissão de *beacons*; comando de MAC, para gerir todos os MACs vizinhos; *acknowledgment* que serve para confirmar a receção do *frame*; e *frame* de dados.

A conexão dos dispositivos à PAN é feita através de *beacons*. Estes são responsáveis por sincronizar os dispositivos, identificar a rede e descrever, no caso de haver, a estrutura da *Super Frame*. A *Super Frame* tem que estar ativa para que possa ser utilizada pelo coordenador como processo de conexão dos dipositivos ao mesmo. No caso de esta estar ativa, o coordenador vai, nos 16 *slots* disponíveis, colocar diversos *beacons* e cada dispositivo se conecta a um. Estando inativa, o coordenador envia apenas um *beacon* e todos os dispositivos se tentam ligar. No caso de haver colisão de *frames*, o CSMA-CA estará ativo, permitindo, assim, que haja tempo de espera após a colisão e a nova tentativa de se conectarem.

A nível de segurança das *frames* faladas anteriormente, é usado o algoritmo de criptografia AES (*Advanced Encryption Standard*). Este algoritmo, e todo o processo, é gerido pela camada MAC, mas as chaves e o nível de segurança são atribuídos pelas camadas mais elevadas. A camada MAC, quando recebe/envia uma *frame*, envia para a origem/destino a chave que será usada.

A integridade de uma *frame* é igualmente importante no que toca à sua transmissão. Esta transmissão, quando ocorre com pedido de integridade, os dados de cabeçalho e do

payload da camada MAC são utilizados para a criação do MIC (Message Integrity Code). Este MIC é inserido no *payload* da camada MAC. No caso de ser ativada, também, a confidencialidade, o *payload* da camada MAC e a sequência são tidos em conta para a encriptação, prevenindo que possam ser intercetados.

2.3.4.3 Z-Wave

O *Z-Wave* é um protocolo *wireless* criado para a transmissão de pequenos pacotes de controlo para um ou mais dispositivos e com o menor ruído possível. (Yassein et al., 2016)

O protocolo obriga a que os dispositivos, que não podem ser mais do que 232, sejam identificados de duas diferentes formas: *Network/Home ID*, que permite que sejam distinguidos dispositivos entre redes *Z-Wave* ou *Node ID*, que permite que os dispositivos sejam distinguidos entre si na mesma rede *Z-Wave*. Usa uma *Mesh Network* que permite que exista um controlador *master*, responsável pelo *routing* e pela segurança. Os dispositivos instalados nesta rede têm a função de cobrir toda a área necessária (de uma casa) e a comunicação entre eles é feita através de nós intermediários. (Z-Wave, 2019)

A comunicação entre dispositivos é feita através de uma frequência rádio, com uma largura de banda de 40 kbit/s e a banda de frequência é a de 900MHz, sendo que estes valores são considerados no melhor desempenho da rede que corresponde a um alcance, entre dispositivos, de 30 metros.

O protocolo é constituído por diversos componentes. Esses componentes passam por controladores (primário e secundário) e *slaves*. Segundo Z-wave, 2019, um controlador é uma unidade que tem a habilidade de compilar uma *routing table* da rede e consegue calcular rotas para diferentes nós da rede.

Neste sentido, existem dois tipos de controladores:

- Primário: este controlador é o principal da rede e apenas pode ser "eleito" em toda a rede. Este é responsável por recolher e armazenar, na *routing table*, toda a informação da rede *Z-Wave* e isso permite que ele controle todos os dispositivos da rede. Também é responsável pela atribuição do *Network/Home ID* e do *Node ID*;

- Secundário: É-lhe atribuído o mesmo *Home ID* que o controlador primário. Este controlador tem como principal função, preservar a *routing table*. Os dados para preencher essa tabela são fornecidos pelo controlador primário.

É importante que ambos os controladores conheçam a topologia da rede, através do uso da *routing table*, pois, assim, conseguem selecionar o melhor caminho para a transmissão de pacotes da origem ao destino.

Por fim, os *slaves* são nós que não têm *routing table* e o seu papel na rede é receber/enviar pacotes e obedecer a comandos enviados pelo controlador primário. O *routing slave* constrói um mapa da rede com todas as informações de diferentes dispositivos, facilitando a sua função de repetidor e permitindo uma melhor decisão no que toca ao melhor caminho origem→destino. É indicado pelo protocolo que o número máximo de *hops* feito pelas mensagens é de cinco, mas o ideal para evitar que a mensagem seja perdida, é dois a três.

O protocolo Z-Wave tem uma arquitetura com as seguintes camadas: Física, MAC, Transporte, *Routing* e Aplicação.

A camada física tem a responsabilidade de gerir e atribuir e permitir a utilização das radiofrequências.

A camada MAC é responsável pela gestão dos *Home ID* e *Node ID* e trata de executar o protocolo de proteção contra colisões nos nós da rede. Esta técnica permite que as *frames* sejam enviadas quando não estão outros nós a comunicar para a rede, caso contrário, a comunicação é adiada por um período aleatório e o processo repetido até ser possível comunicar. Esta camada permite que os nós enviem ACK (*Acknowledgments*) de forma a saber se esse nó está a comunicar ou não. Se não estiver a enviar dados para a rede, os nós comportam-se apenas como recetores de *frames*.

A camada de transferência é responsável por gerir e administrar a conexão entre os nós, tal como a receção e envio de *frames*, a sua retransmissão e os ACK que mostram se a conexão foi bem-sucedida ou não.

A camada de rede é responsável pelo encaminhamento das *frames* pela rede, pela análise da rede e dos componentes nela existentes e de atualizar a *routing table* do controlador primário.

Por fim, a camada de aplicação é a camada responsável pela execução dos comandos presentes no *payload* do *frame*.

2.3.4.4 Wi-Fi

O *Wi-Fi* foi criado em 1997, nasceu do nome "*wireless fidelity*" (Lee) e funciona com base no *standard* IEEE802.11a/b/g. Este protocolo permite, então, que utilizadores/dispositivos possam navegar na internet através da conexão a APs ou módulos *ad hoc*. Segundo (Conference & Systems, 2018), é usada uma frequência de 2.4GHz. No entanto, a mais recente versão do *standard*, IEEE802.11ac usa uma frequência de 5GHz, conseguindo cumprir 1.33GB/s, numa distância máxima de 70 metros. Isto resulta em que seja um protocolo que consome muita energia dos dispositivos.

Uma LAN (*Local Area Network*) em IEEE 802.11 tem uma estrutura chamada de BSS (*Basic Service Set*) que representa um grupo de dispositivos e estações que comunicam entre si. Esta estrutura pode ser representada pelas IBSS (*Independent Basic Service Set*), sendo esta constituída por estações que comunicação entre si, sem necessitarem de APs e pelas ESS (*Extended Service Set*), que são constituídas por diversos BSSs e esses BSSs apenas comunicam através de APs e é usado o componente DS (*Distribution System*).

2.3.4.5 Mobile

Este tópico apresenta diversos protocolos que foram usados ao longos dos anos para permitir comunicações em longa distância. O surgimento do GSM (*Global System for Mobile Communications*) em 1991 (Liikanen et al., 2004) foi o principal ponto de partida para os protocolos de comunicação *mobile* que existem atualmente.

O GSM caracteriza-se pela utilização de transmissão dos sinais e canais de voz digitais, sendo considerado um sistema de segunda geração. O surgimento do 3G permitiu que, para além de voz, pudessem ser enviados e reproduzidos vídeos e o acesso à Internet fosse feito de uma forma mais acessível e rápida. Este protocolo surgiu em 1998 de um projeto com empresas de tecnologia móvel de diferentes cantos do mundo, permitindo a sua implementação a nível global.

A tecnologia 4G/LTE (*Long Term Evolution*) é totalmente baseada em IP. Isto significa que, quando são necessários o envio e a receção de pacotes de dados, vídeo e voz, estes são feitos através de protocolos da internet. Os débitos, geralmente, estão entre os 100Mbps e o 1Gbps e outra vantagem é a diminuição da latência.

A Internet das Coisas, IoT, veio revolucionar o mundo das comunicações móveis e acelerou a criação da mais recente e esperada tecnologia, 5G. Os requisitos para a criação desta tecnologia foram definidos pela ITU-R (*International Telecommunication Union - Radiocommunication Sector*) na Conferência Mundial de Radiocomunicações em 2015. (Souza et al., 2017)

Os requisitos foram definidos com base no esperado aumento de tráfego nos próximos anos. Esses requisitos, entre outros, mencionam dois pontos importantes: capacidade de tráfego e taxa de transmissão de dados e a latência.

Com o aumento de tráfego, a capacidade de tráfego e a taxa de transmissão de dados pode ser afetada e para se conseguir resolver esse problema são instaladas células para pequenas áreas de cobertura. Estas células têm a característica de cobrirem entre dez metros a dois quilómetros e aumentam a taxa de dados em áreas urbanas com um alto nível de congestionamento. (Al-falahy & Alani, 2017)

Este problema também pode ser resolvido com o uso de ondas milimétricas na banda de frequências. Como o espetro já tem as frequências mais baixas em uso, esta solução passa por selecionar intervalos baixos entre ondas de frequência. Por fim, o uso da tecnologia M-MIMO (*Massive Multiple-Input Multiple Output*), juntamente com o *beamforming*, permite que os dados sejam enviados no mesmo canal físico e, juntamente com o aumento do número

de antenas por cada área coberta, permite que a velocidade da transmissão aumente e a banda de frequências seja mais bem utilizada. (Barbosa Cabral, 2017)

Relativamente à latência, o uso de células pequenas permite, também, que a latência desça de 10ms no 4G para 1ms, complementando com o uso de comunicações D2D (*Device to Device*). A comunicação D2D é "*comunicação direta entre dois dipositivos móveis sem passar pela estação base (BS) ou núcleo da rede.*" (Bastos & Cecílio, 2017)

2.3.4.6 NFC

O NFC (*Near Field Communication*) é uma tecnologia que foi criada para comunicações entre dois dispositivos. Os dispositivos não podem estar a mais de 20cm de distância. Esta tecnologia tem como funcionamento base a tecnologia que é usada pelo RFID e o *standard* utilizado é o ISO/IEC 18092 (frequência 13,56 MHz). A taxa de transmissão varia entre os 106, 212, 424 ou os 848 Kbit/s.

O NFC é extremamente simples e tem apenas dois intervenientes numa comunicação - o iniciador e o terminal. Estes dois intervenientes podem fazer parte de duas diferentes formas de comunicação: ativa e a passiva. A comunicação ativa passa por tanto o iniciador como o terminal imitirem sinais RF e um só transmite quando o outro não estiver a transmitir. Ambos os dipositivos costumam ter fontes de alimentação próprias, pois existe um consumo constante de energia. Na comunicação passiva, apenas o iniciador emite sinais RF e apenas existe comunicação quando o terminal se aproxima do iniciador e inicia a transferência dos dados e isto é possível pois o iniciador é constituído por uma antena NFC, classificado de indutor. Quando outro indutor (terminal) de aproxima do iniciador é criado um campo magnético que alimenta o terminal, permitindo que exista energia suficiente para a transmissão dos dados.

2.3.5 Segurança

A segurança em IoT é algo que deve ser tido sempre em conta. Segundo Xu, Wan, & Xue, 2019, os investimentos feitos no design e na implementação de dispositivos IoT em *smart homes* levam a um melhoramento constante da praticidade e do custo, mas nem sempre da segurança e privacidade. Os dispositivos IoT têm cada vez mais tendência a estar ligados à Internet e, por isso, é necessário ter em conta estes contribuintes do bom funcionamento das redes inteligentes.

Segundo Jaouhari, Palacios-Garcia, Anvari-Moghaddam, & Bouabdallah, 2019, é necessário ter em consideração três pontos: a confidencialidade e integridade, a autenticação e o controlo de acesso.

A confidencialidade e a integridade são extremamente importantes no que diz respeito ao transporte de informação pessoal, dos utilizadores - essa informação tem de ser mantida confidencial e apenas poder ser acedida por quem tiver autorização para tal. Os autores Jaouhari et al., 2019 definiram que, na sua prova de conceito usariam o AES128 como protocolo de encriptação.

O AES foi desenvolvido em 1997 e veio substituir o DES (*Data Encryption Standard*). Foi criado para ser de fácil implementação tanto a nível de hardware como de software e capaz de ser usado em diferentes tipos de ambiente/redes. Na prova de conceito mencionada neste parágrafo, os autores optaram por usar o AES128, isto é, encripta e desencripta informação em blocos de 128 *bits*, podendo usar chaves de criptográficas de tamanho variável, 128, 192 ou 256 *bits*. A informação que for transportada é classificada de menos secreta e pode ser usado o AES128 mas quanto mais secreta for, mais blocos serão usados em conjuntos de *bits* por cada chave. No caso de uma chave ser de 128 *bits*, existiriam 10 rondas, 192 *bits*, 12 e, por fim, para 256 *bits*, 14 rondas. Estas rondas consistem num conjunto detalhado de diferentes processos de forma a alterar a forma como a mensagem é transmitida. Neste algoritmo, a chave que encripta a mensagem é a mesma que a desencripta - é um algoritmo de encriptação simétrica.

Outro exemplo de segurança que pode ser utilizada está representada no trabalho dos autores Xu et al., 2019. Neste trabalho é proposto o uso de uma arquitetura ICN (*Information-*

Centric Networking), isto é, uma arquitetura que se preocupa menos com os dispositivos e mais com o conteúdo e a informação que é transmitida entre os dispositivos. Esta arquitetura é caracterizada pela necessidade da existência de *router* ICN que faz a interligação entre as *smart homes* e a Internet. Estes *routers* estarão espalhados por toda a área e serão uma peça fundamental porque, para além de melhorarem a eficiência da distribuição do conteúdo, têm mais memória *cache* e mais capacidade de detetar anomalias nas mensagens que precisem de ser transmitidas entre a Internet e os dispositivos da *smart home* e vice-versa.

O esquema que será usado a nível de segurança é com base na assinatura *proxy*. Este esquema consiste não apenas em criar um campo com uma assinatura digital no pacote de dados (seria demasiado pesado para dispositivos com pouca capacidade de processamento), mas em que o dispositivo IoT tem uma chave privada própria que encripta o pacote de dados que ele enviará com os dados recolhidos e depois, juntamente com o *router* ICN, cria uma assinatura para aquele pacote com base na chave pública desse *router*, garantido, assim, que só aquele *router* pode desencriptar aquela mensagem.

A autenticação é um passo importante quando é necessário aceder a dados presentes numa determinada rede, sendo ainda mais sensível quando se fala de *smart homes*. No trabalho anteriormente mencionado, os autores Jaouhari et al., 2019 mencionaram o uso de um *middleware* de autenticação chamado "*Passport"*. A motivação do uso deste foi o facto de ele ser feito para Node.js, simples de implementar e fornecer diversos modos de autenticação, sendo que a utilizada neste caso em específico é local (*user*, *password*). Para uma autenticação mais robusta aconselham o uso do *OAuth*, um padrão/protocolo que permite que os utilizadores consigam autenticar-se com contas de fornecedores terceiros (*Google*, *Facebook*, etc.).

Por fim, o controlo de acesso é também fundamental no processo de segurança de uma *smart home* pois tem como principal foco proteger a informação (tanto do *frontend* como do *backend*) que é recolhida pelos sensores. Esta informação apenas deve ser acedida por utilizadores autorizados pois pode ser vista, modificada e até mesmo copiada.

Segundo Jaouhari et al., 2019, para um sistema de redes de computadores, são diversos os modelos *standard* de autorização que existem, tais como:

- ACL (*Access Control List*) – lista com a informação dos utilizadores e qual a sua permissão para acesso aos dados. (P. Pfleeger et al., 2015);
- *Access Control Matrix* (ACM) – este modelo de segurança funciona com a relação sujeito/objeto, isto é, para cada par da matriz sujeito/objeto, é dito qual a permissão daquele sujeito/utilizador para ter acesso àquele objeto em específico. (Lampson, 1974). O que difere este Sistema do anterior é a organização dos dados, isto é, os sujeitos estão na coluna da esquerda e os objetos na primeira linha. E para cada objeto existe um sujeito correspondente e esse sujeito só tem as permissões que indicar no cruzamento da coluna com a linha;
- *Multilevel Security* – este sistema permite que cada ficheiro tenha um nível de segurança necessário e são definidos os utilizadores e o que podem ou não fazer em cada um dos ficheiros. (Myers & Liskov, 1997);
- *Role-based access control* (RBAC) – este modelo não se baseia apenas no utilizador e no ficheiro, mas em que funções esse utilizador tem numa determinada rede. Geralmente utilizado em organizações/empresas;
- *Attribute-based access control* – este modelo funciona com base no RBAC e atribui, a cada utilizador, uma característica - essas características são associadas a permissões e objetos previamente definidos. (Al-kahtani & Sandhu, 2002).

2.3.6 Eficiência energética

O consumo de energia tem crescido bastante desde a Revolução Industrial e isso veio influenciar a forma como esta é distribuída. Toda as indústrias, casas e dispositivos utilizam eletricidade para o seu funcionamento, e com o IoT isso não difere. Apesar de os dispositivos assentes em redes IoT consumirem energia, uns mais, outros menos, estes

também podem ser usados para a sua poupança. A eficiência energética é um tema sempre tido em conta no que toca a dispositivos IoT.

Os autores Jaouhari et al., 2019 procederam à implementação de um HEMS (Home Energy Management System) com o objetivo de recolher informações sobre o consumo de energia dos dispositivos locais e otimizar a sua operação.

Esta arquitetura, na camada física, é constituída por tomadas inteligentes, sensores de movimento e *smart meters*. Estes dispositivos utilizam diferentes protocolos de comunicação tais como o *Wi-Fi*, *Bluetooth* e o *ZigBee* e conectam-se à *gateway*. É através dessa conexão que transmitem as informações que recolheram dos diferentes sensores da rede de energia.

Na camada de dados, já são executadas operações mais complexas de forma simultânea. Ao mesmo tempo que a *gateway* recolhe os dados dos dispositivos e os armazena numa base de dados MongoDB, os *smart meters* encriptam a informação.

Na camada de aplicação, o HEMS tem a função de pôr em prática todas as estratégias e correções que serão posteriormente definidas após a receção de dados. As aplicações utilizadas por Jaouhari et al., 2019 utilizam os dados já recolhidos da *smart home*. A primeira aplicação é baseada em LabVIEW e usa os dados recolhidos *on-demand* pelo sistema AMI (Advanced Metering Infrastructure), alarmes feitos pelo sistema de *logs*, eventos ou mau funcionamento. Geralmente, estes dados são mostrados numa interface de fácil uso para o utilizador. A segunda aplicação tem como função recolher os dados relativos à energia e os analisar. Após essa análise, envia pontos/valores de referência que se consideram os ideais e esses valores são recebidos pelos atuadores e controladores mais próximos do dispositivo. Esta aplicação permite também um controlo sobre o desempenho do sistema e a adaptação do mesmo quando as condições são alteradas.

Segundo Jaouhari et al., 2019, o AMI incluí duas camadas, a camada física e a camada utilitária. A camada física é constituída por medidores inteligentes e o concentrador de dados que permitem fazer a recolha das medições feitas periodicamente, sendo que estes dados, devidamente classificados, são enviados para um servidor NTP (*Network Time Protocol*). A camada utilitária é constituída pelo software lógico fornecido pelo Kamstrup, o OMNIA.

Este *software* utiliza *Ethernet* para se comunicar com o concentrador de dados e implementa todos os processos necessários para gerir o sistema e fazer as leituras periódicas necessárias.

2.3.7 Alertas

Os alertas são uma peça fundamental no que toda à monitorização. São as ferramentas que permitem que, com a informação recolhida pelos sensores, as pessoas possam ser avisadas de quando algo está errado com os dispositivos ou a rede.

No contexto da IoT é importante mencionar que os sensores são usados como leitores do ambiente em que se inserem e, por isso, são uma peça fundamental para a recolha dos dados necessários. Os dados terão de ser recolhidos em tempo real e terão de ser definidos intervalos de valores para que possa ser gerado o alerta. Os valores dependem de que sensor se trata.

O tipo de sensor e o seu objetivo define, praticamente, o que será feito com os dados que recolhe, isto é, quanto mais o ambiente em que esse sensor é inserido, mais alertas terão de existir de forma a que possam agir a tempo no caso de haver algum problema.

No trabalho dos autores Saha & Majumdar, 2017, o ambiente a ser monitorizado é um *data centre*. Esta rede WSN é constituída por sensores de temperatura, um ESP8266 e um *router Wi-Fi*. Na sala estão inseridos dois sensores e são recolhidos os dados desses dois sensores e os dados são sempre comparados de forma a verificar a sua veracidade. Os dados que são recolhidos pelo sensor são enviados para o ESP8266 que os analisa e, ao existir uma conexão *Wi-Fi* direta entre o AP (*router Wi-Fi*), eles são diretamente enviados, e em tempo real, para a plataforma *Ubidots* (Ubidots, 2020) . A configuração de alertas é extremamente importante tendo em conta a sensibilidade do ambiente em que este sensor se insere. No trabalho, foram criados na plataforma apenas dois tipos de alerta: SMS (Short Message Service) e e-mail. A plataforma tem mais opções de alertas: *Webhook*, *Telegram* e *Slack*.

2.4 Gestão do Risco

Segundo o Quadro Nacional de Referência para a Cibersegurança (QNRCS) (Centro Nacional de Cibersegurança, 2019) e com origem na lei 46/2018, art.3º, al. n, o risco é *"uma circunstância ou um evento razoavelmente identificável, com um efeito adverso potencial na segurança das redes e dos sistemas de informação"*. (Assembleia da República, 2018a)

É imperativo gerir todos os riscos numa organização. A gestão do risco é constituída por "*atividades coordenadas para dirigir e controlar uma organização…*" (Centro Nacional de Cibersegurança, 2019) e o impacto da mesma influencia e põe em causa a "*garantia da confidencialidade, disponibilidade e integridade*" (Centro Nacional de Cibersegurança, 2019) na prestação de serviços e comercialização de bens. A gestão do risco organizacional passa pela execução de um exercício sistematizado que permite avaliar, identificar e categorizar possíveis vulnerabilidades dos ativos e as ameaças que podem recair sobre essas vulnerabilidades.

De acordo com o autor, ao longo do documento, "*são propostas diversas abordagens ao processo de avaliação periódica dos riscos*" (Centro Nacional de Cibersegurança, 2019). Estas avaliações têm como objetivo permitir que a organização possa definir os critérios e necessidades atuais a nível de cibersegurança.

O risco e a gestão do risco são extremamente importantes em qualquer empresa. Para padronizar as boas práticas de segurança existem diversas orientações, a começar pelo ISO 31000:2018 (versão mais recente). Segundo a ISO, 2018, este documento permite que as organizações se possam orientar em todas as tomadas de decisões, tendo sempre em consideração o planeamento, a gestão, os relatórios, políticas, valores e a cultura dessa mesma organização.

O mesmo autor indica que a implementação do ISO 31000 ajuda as organizações a identificar as suas oportunidades e as consequências associadas ao risco. Para isso, é necessário que as organizações desenvolvam uma estratégia de gestão dos riscos para identificar e mitigar, efetivamente, os riscos, para que possam atingir os seus objetivos.

O ISO/IEC 27032:2012 (ISO/IEC, 2012) (versão mais recente) é um documento focado em orientações destinadas a melhorar o estado da segurança cibernética, tendo em consideração diversos tipos de contextos, tais como: a segurança da informação, a segurança da rede, a segurança na internet e a proteção de toda a infraestrutura tecnológica crítica. Segundo ISO, 2012, este documento abrange, entre diversas recomendações básicas de segurança, uma visão geral da *Cibersecurity*, uma explicação da relação entre a cibersegurança e os outros tipos de segurança, a definição dos *stakeholders* e qual o seu papel na cibersegurança, um guião para a resolução de problemas comuns na cibersegurança e, por fim, uma estrutura que permita que os *stakeholders* colaborem na resolução de problemas na cibersegurança.

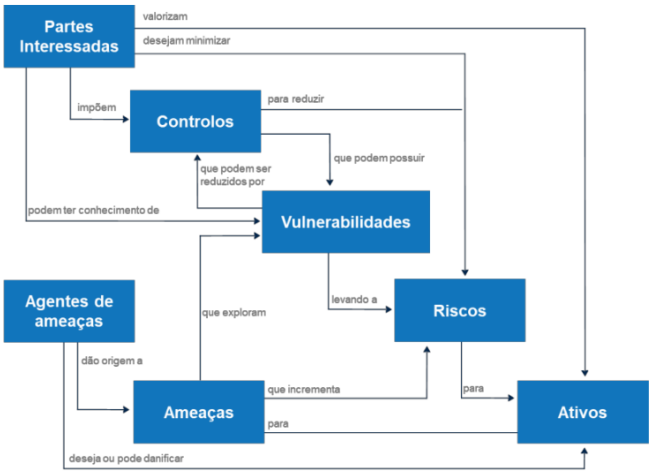


Figura 9 – ISO/IEC 27032 – Conceitos básicos e relações de alto nível (Centro Nacional de Cibersegurança, 2019)

O ISO/IEC 27005:2018 (ISO/IEC, 2018a) (versão mais recente) é um documento igualmente importante por abranger a gestão de riscos dos sistemas de informação de uma organização. O documento criado pela ISO e a IEC fornece diretrizes para a gestão dos riscos, sendo que não mostra às organizações métodos específicos, ficando nas mãos da mesma definir qual a abordagem. A definição da abordagem deverá ser feita com base num sistema de gestão da segurança da informação, no contexto da gestão dos riscos e do setor de atividade da organização.

Figura 10 – ISO/IEC 27005 – Fases da Gestão do Risco dos Sistemas de Informação
(Centro Nacional de Cibersegurança, 2019)

Na Figura 10 estão representadas as fases da gestão do risco, isto é, todas as fases necessárias para a criação e execução de um processo de gestão do risco numa determinada organização.

Segundo Patino et al., 2018, em primeiro lugar é feito um contexto da organização, isto é, a recolha de toda a informação relativa à empresa que seja importante para a identificação dos seus riscos. Após a organização estabelecer esse contexto, inicia-se o processo de avaliação do risco. Como está representado na figura 10, a avaliação de risco passa por três fases: identificação, análise e evolução. É necessário que estas três fases consigam ser cumpridas para que a avaliação de risco seja satisfatória. Caso contrário, o processo terá de ser novamente iniciado. O tratamento do risco é um processo que aplica medidas para a alteração do risco em causa. "*The effectiveness of risk treatment depends on the results of the risk assessment.*" (Patino et al., 2018). Os riscos têm de ser aceites por todos os intervenientes do processo.

2.4.1 Estabelecer contexto

2.4.1.1 Organização na gestão do risco

A execução do processo de gestão do risco é influenciada pela identificação, por parte da organização, dos recursos humanos e materiais.

Para a correta execução desse mesmo processo de gestão do risco, a organização deve definir (Centro Nacional de Cibersegurança, 2019):

- Metodologias de gestão do risco adaptadas à realidade da organização;
- As partes interessadas, tanto internas como externas;
- Responsabilidades/papéis internos e externos na gestão do risco e a sua atribuição (por exemplo Gestor do risco, Membro da equipa de gestão do risco);
- Ferramentas para suportar a gestão e o tratamento do risco; e
- Os registos a criar/manter, tais como atas de reuniões e relatórios de progresso.

2.4.1.2 Abordagem à gestão do risco

Em conjunto com o ponto 2.4.1.1, a organização deve definir quais os recursos que vão permitir:

- "*Poder definir e implementar as políticas, processos e procedimentos no âmbito da gestão e tratamento do risco;*
- *Poder efetuar o levantamento e o plano de tratamento dos riscos;*
- *Poder efetuar a monitorização dos controlos implementados;*
- *Poder efetuar o acompanhamento da eficácia da implementação do plano de tratamento do risco.*" (Centro Nacional de Cibersegurança, 2019)

2.4.1.3 Critérios de avaliação do risco

A identificação da relevância do risco na organização está diretamente dependente da definição de critérios de avaliação do risco. Essa definição deverá ser feita com base no nível

de criticidade dos ativos, no valor estratégico dos processos que caracterizam o negócio da organização, nas expectativas/avaliações das partes interessadas e, por fim, na importância operacional/comercial no que diz respeito à confidencialidade, integridade e disponibilidade da informação.

Se a organização achar por bem, poderá identificar mais critérios de avaliação que poderão alterar a priorização do tratamento dos riscos.

2.4.1.4 Critérios de impacto

A gestão do risco deverá ser suportada por níveis de impacto. Esses níveis de impacto devem ser definidos pela organização e, quando associados ao risco, devem ser considerados os seguintes critérios: a importância/classificação dos ativos para a organização, as possíveis falhas na segurança da informação (integridade, confidencialidade e disponibilidade da mesma), a alteração de todo o planeamento e prazos da organização, os custos totais e extra que a organização terá de suportar e, por fim, os danos causados na imagem e na reputação da organização.

2.4.1.5 Critérios de aceitação do risco

A organização terá de identificar a partir de que nível do risco a mesma deve aceitá-lo. Essa possível aceitação terá de ser analisada pela gestão de topo para que possa ser considerada válida. A organização, ao identificar os critérios de aceitação do risco, deve considerar diversos fatores, tais como: operacionais, tecnológicos, financeiros, sociais e humanitários.

A definição dos critérios de aceitação do risco passa pelos seguintes pontos (Centro Nacional de Cibersegurança, 2019):

- Definição de um nível do risco aceitável sendo que, acima desse nível, a aceitação do(s) risco(s) deve ser formalmente feita pela gestão de topo;
- Definição de requisitos específicos relativamente ao futuro daquele risco, sendo que pode ficar acordado que, apesar da aceitação do(s) mesmo(s), serão

tomadas medidas num determinado período para a redução para níveis aceitáveis.

- Por fim, como o risco pode ser resultado de uma atividade temporária, ou de curto prazo na organização, os critérios de aceitação deverão se adaptar ao tempo de vida desse mesmo risco.

2.4.1.6 Definição de âmbito e fronteiras

É importante identificar-se o âmbito e as fronteiras do sistema de gestão do risco pois a organização conseguirá identificar, na fase de levantamento, quais os ativos relevantes para e agregar riscos que tenham sido identificados nessas mesmas fronteiras.

A definição do âmbito num processo de gestão do risco passa pela organização identificar, por exemplo, o edifício, a sua localização, as plataformas de infraestrutura e os processos associados à sua atividade.

Por fim, é importante a organização, na definição em causa neste ponto, ter em conta variáveis como: os seus objetivos estratégicos, as funções e estrutura interna, as políticas de segurança da informação já aplicadas, os ativos de informação, as expectativas das partes interessadas (internas e externas) e o seu âmbito sociocultural.

2.4.2 Identificação do risco

Segundo o Centro Nacional de Cibersegurança, 2019, a identificação do risco é a primeira fase da etapa de levantamento dos riscos. Esta fase permitirá "*identificar, reconhecer e descrever os riscos*" (Centro Nacional de Cibersegurança, 2019) que possam colocar entraves à conclusão dos objetivos da organização. O objetivo principal desta fase do processo é determinar que ocorrências podem provocar uma perda à organização.

2.4.2.1 Identificação dos ativos

"*Os ativos são tudo o que tem valor e que requer proteção na ótica da organização.*" (Centro Nacional de Cibersegurança, 2019)

Para uma organização, os ativos podem pertencer a uma ou mais categorias, das quais se destacam as seguintes quatro: Recursos Humanos, Localizações, Dispositivos de rede, Tecnológicos.

Na prática, a organização deve identificar e inventariar os seus ativos com o maior número de informação possível. Essa informação, segundo (Centro Nacional de Cibersegurança, 2019), no mínimo será:

- "*O número de inventário do ativo;*
- *Uma descrição das funções dos mesmos;*
- *A identificação do responsável;*
- *A sua localização;*
- *Categoria/tipo;*
- *Classificação do ativo de acordo com a sua criticidade para a organização;*
- *Identificação dos processos referentes à atividade da organização que os ativos suportam;*
- *Identificação de dependências com outros ativos.*"

2.4.2.2 Identificar ameaças

Segundo Paulsen, C. Toth, 2016, uma ameaça é algo que pode afetar de forma adversa as informações que a organização precisa para praticar o seu negócio. Uma ameaça, seja de origem natural ou humana, tem um impacto negativo e consequências igualmente negativas nos ativos da organização.

As ameaças mais comuns, segundo o mesmo autor, têm origem:

- Ambiental (por exemplo incêndios, inundações, tornados, terramotos, etc);

- Nos recursos necessários para a atividade da organização, isto é, falhas em equipamentos, interrupção da cadeia de fornecimento ou até mesmo os funcionários; e
- Nos chamados *Hostile Actors*, que são, entre outros, *hackers*, *hacktivists*, criminosos e *nation-state actors*. De salientar que o termo *hackers*, neste contexto, é usado erradamente porque, por definição é aplicado a pessoas que apenas têm vontade de aprender e explorar, sem qualquer intenção criminosa. O termo correto é *crackers*.

A organização poderá detetar a presença de ameaças com recurso a diferentes métodos e entidades, tais como:

- "*Revisão de incidentes ocorridos*";
- "*Responsáveis pelos ativos*";
- "*Utilizadores*" da rede da organização que possam detetar alguma anomalia;
- "*Especialistas de segurança da informação e de segurança física*";
- "*Departamentos legais*"; e
- "*Catálogo de ameaças*", em que a organização poderá, dependendo da avaliação do risco atual, fazer um estudo mais específico à sua área de negócio.

2.4.2.3 Identificar controlos

Aos planos de gestão do risco anteriormente definidos, deverão estar associados os controlos que cada plano deverá implementar. É importante sempre a respetiva identificação do estado da implementação e a utilização desses mesmos controlos.

A análise dos anteriores planos de segurança da informação é fundamental para o conhecimento do que está atualmente implementado. Essa análise passa pelas seguintes ações:

- Revisão dos documentos que suportam estes planos que, se bem feitos no passado, terão neles informações sobre os controlos planeados/implementados e qual a sua fase de implementação.
- Confirmação dos controlos já implementados junto das pessoas responsáveis pela segurança da informação, como por exemplo CISO (*Chief Information Security Officer*) ou, mais recentemente, DPO (*Data Protection Officer*) e o COO (*Chief Operating Officer*); e
- Por fim, deverá verificar-se se os controlos listados como implementados no plano de segurança estão verdadeiramente implementados e operacionais.

Em conclusão, a lista de controlos da organização deverá ser devidamente atualizada, onde deverão constar os controlos já existentes e os planeados, e qual o estado de implementação de cada um.

2.4.2.4 Identificação de vulnerabilidades

A identificação das vulnerabilidades também é importante para a organização perceber o que pode realmente causar danos na sua atividade. A lista das vulnerabilidades deverá ser criada com base nas listas de ameaças, ativos e controlos implementados. É importante entender que as vulnerabilidades não causam danos por si só, mas a sua associação a uma ameaça pode resultar em consequências graves para a organização.

As vulnerabilidades deverão ser monitorizadas e controladas pela organização, tal como os controlos implementados. Isto porque, se os controlos não estiverem bem implementados ou em total operacionalidade, poderão tornar-se em vulnerabilidades

2.4.2.5 Identificação de impacto

A identificação das vulnerabilidades é fundamental para que o impacto possa ser identificado. As vulnerabilidades, ao serem exploradas por uma possível ameaça, põem em causa a confidencialidade, integridade e/ou disponibilidade dos ativos da organização que

tenham sido anteriormente identificados como críticos e, assim, inseridos no processo de gestão do risco. Os ativos devem ser classificados com base no valor para a organização e nas consequências que o seu dano pode causar para o negócio da organização.

As ameaças que podem surgir da exploração das vulnerabilidades podem originar um ou mais cenários de incidentes. Esses cenários de incidente devem ser determinados com base nos critérios de impacto, definidos no ponto 2.4.1.4.

Em suma, a identificação do impacto é feita com base nas vulnerabilidades e nas ameaças a elas associadas, mas também devem ser analisadas as consequências que as mesmas podem ter nos ativos considerados críticos para o negócio da organização.

A organização deverá identificar as consequências operacionais resultado do(s) incidente(s), tais como: tempo de investigação do impacto e a execução das reparações necessárias (o que reduz no tempo disponível por parte da organização para outras tarefas e aumenta os gastos), a perda de oportunidades, os possíveis danos na sua reputação e a segurança e saúde de toda a organização.

2.4.3 Análise do risco

A análise do risco por parte de uma organização deve ter em consideração: "*incertezas, fontes do risco, consequências, eventos, cenários, controlos e a sua eficácia.*" (Centro Nacional de Cibersegurança, 2019)

Segundo o Centro Nacional de Cibersegurança, 2019, um evento pode ter diversas causas, sendo que as mesmas podem criar consequências que afetam um ou mais objetivos da organização ou até mesmo a sua missão e reputação.

O processo de análise ao risco deve ser dividido em diversos níveis de forma a abranger fatores como a criticidade dos ativos, as vulnerabilidades atuais e das ameaças a elas associadas e de todos os incidentes que possam ter acontecido até ao momento.

No seguimento dos pontos 2.4.1.4 e 2.4.2.5 e em conjunto com a análise do risco, é importante a organização, na definição dos critérios do impacto do risco, ter em atenção áreas como:

- Reputação da organização: é preciso ter em conta a importância da confiança das partes interessadas na organização;
- Legal/Regulatória: é importante a organização não permitir que um evento/incidente possa pôr em causa quaisquer responsabilidades legais/regulatórias da mesma;
- Serviço prestado a clientes: a organização terá de garantir que nenhum evento/incidente possa afetar o serviço prestado aos clientes, não cumprindo com o nível de serviço estipulado; e
- Financeira: a ocorrência de eventos/incidentes poderá afetar a estabilidade financeira da organização pois pode ter custos financeiros acima do previsto.

2.4.3.1 Metodologia de análise

A metodologia de análise do risco pode ser constituída por três tipos de análise: qualitativa, quantitativa ou uma combinação das duas. O método de análise definido pela organização deverá ir de encontro aos critérios de avaliação na fase de definição de contexto do risco.

Segundo o Centro Nacional de Cibersegurança, 2019, no início desta metodologia as organizações optam pela utilização da análise qualitativa do risco, pois esta permite uma melhor compreensão dos indicadores do risco. No entanto, pode ter como desvantagem a subjetividade da escala utilizada.

Na análise qualitativa é criada uma escala de qualificação de forma a identificar o perigo dos potenciais impactos e a probabilidade dessas mesmas ocorrências. O risco é definido através da fórmula Risco = Impacto x Probabilidade.

A análise quantitativa deverá ser feita com base numa escala de valores numéricos. Esta é uma análise que terá de ter uma extrema precisão nos dados pois, caso contrário, poderá criar uma falsa sensação de confiança na eficácia do processo de avaliação do risco. Por fim, os valores utilizados nestas análises são baseados em dados de histórico de incidentes.

2.4.3.2 Levantamento dos impactos

O levantamento dos impactos é apenas possível se, anteriormente, tiverem sido identificadas as ameaças, as vulnerabilidades e os ativos que poderão ser afetados por alguns incidentes, comprometendo a integridade, confidencialidade e disponibilidade dos mesmos. Deve também avaliar-se o impacto desses mesmos incidentes nos serviços prestados pela organização. Como referido anteriormente, o impacto dos incidentes deve ser avaliado em perspetivas financeiras, legais e até mesmo de reputação a organização, entre outras.

2.4.3.3 Análise de probabilidade

A probabilidade da ocorrência do risco deve ser calculada com base nos seguintes fatores: ameaças, vulnerabilidades, incidentes anteriores e lições aprendidas nesses mesmos incidentes.

A identificação dos cenários de incidentes deve incluir: ameaças identificadas e qual a sua frequência e origem (humana ou acidental), as vulnerabilidades envolvidas e facilidade com que podem ser exploradas, os ativos prejudicados e, por fim, o impacto deste(s) incidente(s) nos processos diretamente ligados à atividade da organização.

2.4.3.4 Determinação do nível do risco

Este ponto toca na fórmula apresentada no ponto 2.4.3.1, sempre reforçando a ideia de que é necessário que todos os riscos, independentemente do método de análise utilizado pela organização, devem ter-lhes atribuído um nível.

2.4.4 Avaliação do risco

No ponto 2.4.1.3, na definição do contexto, a organização terá de ter descrito os critérios de avaliação dos riscos. A avaliação do risco é necessária para que a organização reveja as definições anteriormente feitas, permitindo conhecer mais informação sobre os riscos identificados.

A avaliação do risco deverá permitir, para além da revisão do processo de estabelecimento do contexto da organização, consolidar toda a informação sobre os níveis do risco, os impactos, as vulnerabilidades e também a confiança depositada na identificação/análise do risco.

Como sugerido pelo Centro Nacional de Cibersegurança, 2019, a junção de riscos com diferentes níveis poderá originar riscos "comuns" mais elevados. Na avaliação do risco, a organização poderá criar uma lista dos riscos para que possam ser agrupados, nunca esquecendo que a sua ordem deve ser feita com base nos critérios de avaliação e os cenários de incidentes que originaram os riscos já identificados.

E de forma a concluir a fase de levantamento do risco, na Figura 11 é demonstrada a relação entre as ameaças, as vulnerabilidades, as probabilidades e o impacto.

As ameaças exploram as vulnerabilidades - a probabilidade dessa ameaça afetar a atividade da organização deve ser avaliada e, logo de seguida, deve avaliar-se o impacto dessa ação, obtendo-se como resultado a obtenção do Risco.

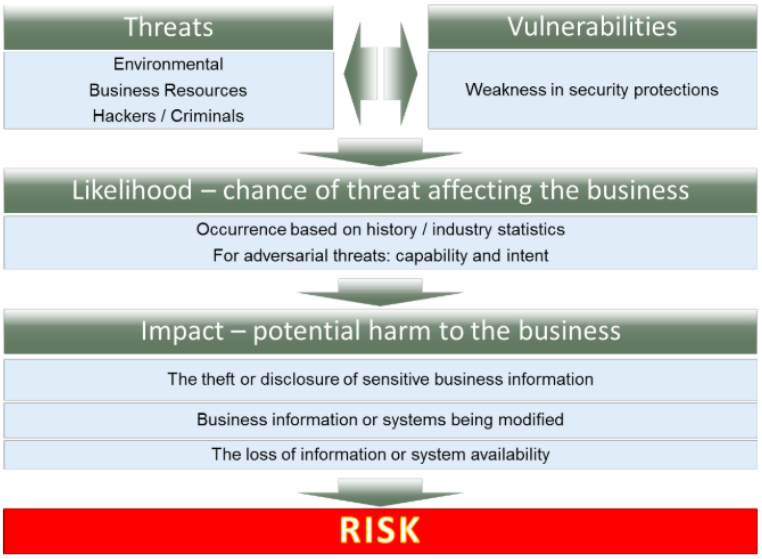


Figura 11 – Relação entre Ameaças, Vulnerabilidades, Probabilidades e Impacto
(Paulsen, C. Toth, 2016)

2.4.5 Tratamento do risco

O plano de tratamento do risco deve ser definido pela organização após a mesma identificar qual o melhor tratamento do risco e, posto isto, identificar quais os controlos que vão aplicar uma das quatro opções do tratamento do risco:

- "*Evitar o risco: Colocar a probabilidade ou impacto tendencialmente próximo de zero, tornando mais difícil a sua ocorrência e/ou eliminar totalmente o seu impacto;*
- *Aceitar o risco: Decisão de aceitação do risco. A assunção de responsabilidade por essa decisão deve ser formalmente registada pela organização;*
- *Mitigar o risco: Reduzir a probabilidade e/ou impacto de um evento adverso para limites aceitáveis através da implementação de controlos ou contramedidas;*
- *Transferir o risco: Transferir, total ou parcialmente, para terceiras partes, o impacto em relação a uma ameaça (por exemplo: efetuar a contratualização de um seguro).*" (Centro Nacional de Cibersegurança, 2019)

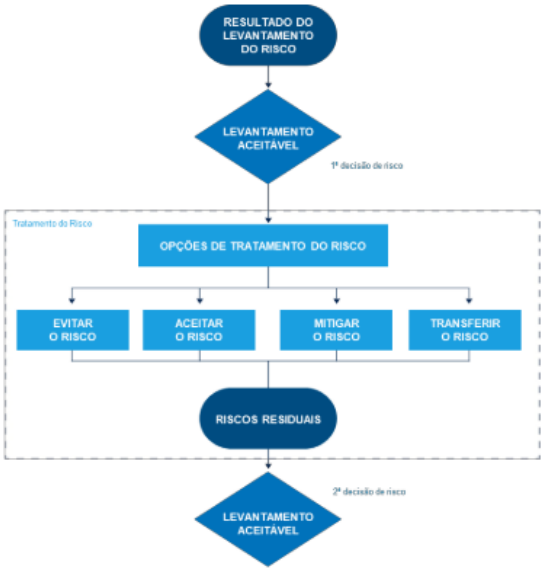


Figura 12 – ISO/IEC 27005 – Tratamento do Risco (Centro Nacional de Cibersegurança, 2019)

Na Figura 12 está descrito o percurso após o resultado do levantamento do risco. Se o levantamento do risco é aceitável, são identificadas as opções de tratamento do risco, em que a organização deve saber como as suas partes interessadas interpretam o risco e a forma mais adequada de comunicar com as mesmas. Após a escolha de qual tratamento do risco executar, vem a determinação dos riscos residuais. Por fim, se todas as etapas forem concluídas, será determinado que foi feito um levantamento aceitável.

No caso de este ter uma resposta negativa, voltará à fase de estabelecer contexto e terá de se repetir o processo até que fique tudo bem identificado e definido, tal como mostra na Figura 10 (Fases da Gestão do Risco dos Sistemas de Informação).

2.4.6 Comunicação e consulta do risco

A comunicação e consulta do risco deverá ser feita independentemente do tratamento do risco escolhido. A organização deve comunicar às suas partes interessadas toda a

informação referentes aos riscos. Esta comunicação deverá ser contínua e feita com base em planos de comunicação que suportem os processos do risco comuns e de emergência.

A comunicação deve ser feita com os seguintes objetivos (Centro Nacional de Cibersegurança, 2019):

- Garantir o resultado da gestão dos riscos definida e implementada pela e na organização;
- Compilar informações sobre o risco e também os resultados da avaliação do mesmo;
- Apresentar o plano de tratamento dos riscos;
- Melhorar o entendimento entre quem toma as decisões e as partes interessadas, de forma a reduzir/evitar o impacto das quebras de segurança da informação;
- Aprender mais sobre as temáticas de segurança da informação na organização;
- Planear, juntamente com as partes interessadas, respostas para reduzir o impacto dos incidentes;
- Demonstrar a responsabilidade sobre os riscos a quem toma as decisões e às partes interessadas da organização;
- Intensificar a importância do processo de gestão dos riscos.

2.4.7 Monitorização e revisão do risco

A monitorização e revisão do risco deve ser feita com regularidade, de forma a que possam ser detetadas rapidamente alterações que possam influenciar o contexto da organização e, consequentemente, a perceção do risco.

Os pontos que deverão ser monitorizados continuamente pela organização são:

- Ativos novos inseridos no processo de gestão do risco;
- Mudanças na criticidade dos ativos;
- Novas ameaças, não avaliadas, com origem dentro ou fora da organização;
- Novas vulnerabilidades, sendo que as mesmas podem ser exploradas também por essas novas ameaças;

- Alterações do impacto, alterando assim o nível do risco;
- Outros incidentes de segurança que podem ocorrer.

2.4.8 *Cybersecurity Framework Version* 1.1 (NIST, 2018)

Segundo NIST, 2018, esta *framework* tem como foco o uso de orientações de negócio para direcionar a organização quanto às atividades de cibersegurança e a consideração da mesma pelos riscos de cibersegurança nos processos de gestão do risco da organização. Esta *framework* permite às organizações, independentemente do seu tamanho, nível do risco de cibersegurança ou sofisticação, que possam aplicar as melhores práticas de gestão do risco para a melhoria da segurança e da resiliência.

A *framework*, com a sua abordagem à gestão do risco, é composta por três partes: *The Framework Core*, *Framework Implementation Tiers* e *Framework Profile*.

2.4.8.1 Framework Core

A *Framework Core* sugere à organização um conjunto de atividades que vai permitir que a organização consiga alcançar determinados objetivos na cibersegurança. É importante salientar que não é necessário a organização seguir na totalidade as atividades propostas por esta ferramenta. Esta fase é constituída por quatro elementos: Medidas de Segurança, Categorias, Subcategorias e Referências.

Na Figura 13 está um pequeno exemplo da estrutura definida por esta mesma fase. Na Figura 14 está representada a estrutura base do QNRCS, sendo evidentes as semelhanças entre as mesmas.

Figura 13 – *Framework Core* (NIST, 2018)

Objetivos	Medidas de Segurança					
IDENTIFICAR	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas
PROTEGER	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas
DETETAR	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas
RESPONDER	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas
RECUPERAR	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas

Figura 14 – Estrutura base do QNRCS (Centro Nacional de Cibersegurança, 2019)

2.4.8.2 The Framework Implementation Tiers

Esta segunda parte é a que permite entender como a organização olha para o risco na cibersegurança e quais os processos em execução para a gestão desse risco. Este conceito divide-se em quatro níveis: *Tier 1* (*Partial*), *Tier 2* (*Risk Informed*), *Tier 3* (*Repeatable*) e *Tier 4* (*Adaptive*).

A organização deverá identificar o seu nível com base nas práticas implementadas no momento de gestão do risco, no ambiente de ameaças, nos requisitos legais e regulamentares, nos hábitos/práticas de partilha de informação e no(s) objetivo(s) da organização e da sua atividade. Os níveis não representam a maturidade da organização, apenas se destinam a apoiar as tomadas de decisões por parte da organização sobre a gestão do risco ma cibersegurança.

No *Tier 1,* relativamente ao processo de gestão do risco, a organização encontra-se numa posição de práticas não normalizadas, sendo que o risco muitas vezes é gerido de modo *ad hoc* e não são tidos certos aspetos em conta como os objetivos da organização e da sua atividade/negócio e/ou o ambiente atual de ameaças. No programa integrado de gestão do risco, não há uma implementação constante da gestão do risco (apenas quando necessário) e não estão em execução processos de partilha de informação sobre a cibersegurança dentro da organização. Por fim, na participação externa da organização, a mesma não entende qual o seu papel no ecossistema em que se insere, não partilha nem recebe informações (melhores práticas, tecnologias, evolução das ameaças, etc) de outras entidades (fornecedores, clientes, entidades governamentais, etc) e na maioria das vezes não tem conhecimento dos riscos de cibersegurança do que contrata ou fornece.

No *Tier 2*, no processo de gestão do risco, a organização implementa práticas aprovadas pela gestão de topo, mas não são definidas como políticas para toda a organização. As atividades de cibersegurança e a necessidade de proteção são diretamente influenciadas pelos objetivos da organização ou da sua atividade/negócio. No programa integrado de gestão do risco, as informações relativas à cibersegurança são partilhadas de informalmente dentro da organização e não são tidas em conta nos processos organizacionais. Por fim, a participação externa, a organização entende o seu papel no ecossistema em que se insere, colabora e recebe informação de outras entidades, mas não pode partilhar informações com outros e está ciente dos riscos de cibersegurança do que fornece ou contrata, mas não toma medidas formais para combate a esses riscos.

No *Tier 3*, o processo de gestão de risco é aplicado com a execução de práticas aprovadas e expressas como políticas. Com base nas mudanças das necessidades da atividade/negócio da organização, as práticas de cibersegurança são atualizadas com regularidade. No programa integrado de gestão do risco são definidas e divulgadas políticas, processos e procedimentos com base no conhecimento dos riscos, existem métodos de resposta à alteração dos riscos, existe pessoal qualificado para o cumprimento das responsabilidades na cibersegurança, a organização monitoriza e identifica os ativos críticos, os colaboradores comunicam regularmente sobre os riscos que possam ser identificados e os executivos garantem a valorização da cibersegurança em todas as linhas de operação da organização. Por fim, na participação externa da organização, a mesma entende o seu papel no ecossistema, os seus dependentes e dependências, e contribui de forma mais intensa para o conhecimento sobre cibersegurança por parte da comunidade.

No último nível, o *Tier 4*, relativamente ao processo de gestão do risco, a organização adapta as suas práticas de cibersegurança com base nas atividades anteriores e atuais, incluindo lições aprendidas e indicadores previamente previstos. A organização usa um processo de melhoria continua com tecnologias e práticas avançadas para se adaptar ativamente a cenários de ameaças e alterações de tecnologias e, no caso das ameaças, responde de forma oportuna. No programa integrado de gestão do risco, a organização, na sua totalidade, adota políticas, processos e procedimentos sobre riscos previamente detetados e potenciais eventos de cibersegurança. Na tomada de decisões, a organização tem bem definida a relação entre os riscos e os objetivos organizacionais. Os executivos monitorizam os riscos de cibersegurança de forma similar aos riscos financeiros ou outros riscos organizacionais considerados essenciais para a organização. O orçamento da organização é baseado na compreensão dos riscos atuais e na tolerância a esses mesmos riscos. A organização pode rapidamente contabilizar as mudanças nos objetivos/missão com base na forma como o risco é abordado e comunicado. Por fim, na participação externa da organização, a mesma entende o seu papel, dependências e dependentes no ecossistema e

contribui para o entendimento mais amplo sobre os riscos por parte da comunidade. À medida da evolução dos cenários de ameaças e da tecnologia, a organização recebe, gera e analisa informação contínua sobre os seus riscos e partilha-a interna e externamente. A organização usa informações em tempo real para agir consistentemente sobre os riscos nos ativos críticos da organização. Além disso, comunica de forma proativa, utilizando mecanismos formais como acordos e informais, mantendo uma relação forte com outras entidades.

2.4.8.3 Framework Profile

A última parte passa por interligar as Medidas de Segurança, Categorias e Subcategorias com os objetivos de negócio, a tolerância ao risco e os recursos da organização. A definição de um Perfil vai permitir à organização estabelecer um guia para reduzir o risco na cibersegurança. Este guia deve estar devidamente consolidado com as metas da organização, os requisitos legais/regulamentares e deve indicar as prioridades para a gestão do risco. As organizações podem tornar-se/ser complexas permitindo, assim, que a mesma organização tenha vários perfis, alinhados com componentes específicos e reconhecendo as suas necessidades individuais.

Os Perfis definidos podem ser utilizados para descrever o estado atual ou o estado alvo desejado das atividades específicas de cibersegurança. O Perfil Atual demonstra os resultados de cibersegurança que estão a ser alcançados atualmente. O Perfil Alvo indica os resultados necessários para atingir as metas desejadas no que diz respeito à gestão do risco na cibersegurança. A implementação destes mesmos Perfis é feita de forma individual pela organização, sendo que esta *framework* não apresenta modelos de Perfis.

A comparação de ambos os perfis pode permitir a revelação de falhas que devem ser abordadas para garantir o cumprimento dos objetivos da gestão do risco na cibersegurança. A mitigação destas falhas poderá ser feita com um plano de ação que faça cumprir uma determinada Categoria ou Subcategoria. A prioritização da mitigação destas falhas é definida com base nas necessidades do negócio/atividade da organização e dos processos de gestão do risco. A abordagem com base no risco vai permitir que a organização fique com uma

noção dos recursos que poderá necessitar para atingir as metas de cibersegurança de forma rápida e o mais económica possível.

2.4.8.4 Implementação da Framework

No NIST, 2018 são sugeridos sete passos para a implementação desta *framework* numa organização. Esta *framework* vai ajudar a organização a criar um programa de cibersegurança ou até mesmo a melhorar o programa atualmente implementado.

Os sete passos deverão ser repetidos sempre que for necessária uma melhoria da cibersegurança e esses passos são os seguintes:

- **Passo 1: Prioridade e Alvo** – a organização tem de identificar os objetivos do negócio e da sua missão e as prioridades de alto-nível. Com esta informação a organização pode determinar qual o alvo da cibersegurança e quais os sistemas e ativos que suportam o negócio/missão da mesma. Esta *framework* poderá ser adaptada a linhas de negócio ou a processos específicos dentro da organização com uma tolerância ao risco dedicada;
- **Passo 2: Orientação** – uma vez que o alvo do programa de cibersegurança está identificado, a organização tem de identificar os sistemas e ativos relacionados, os requisitos regulamentares e a abordagem ao risco. A organização deve consultar fontes para identificar ameaças e vulnerabilidades possíveis de serem aplicadas aos sistemas e ativos identificados;
- **Passo 3: Criação do Perfil Atual** – o Perfil Atual é criado pela organização com base nos resultados das Categorias e Subcategorias da *Framework Core*;
- **Passo 4: Condução de uma avaliação do risco** – esta avaliação pode ser direcionada pelo processo geral de gestão do risco da organização ou atividades anteriores. O ambiente organizacional deve ser analisado pela organização para que possa distinguir a probabilidade de um evento e o impacto que esse evento poderá ter na organização. Esta análise vai ser mais

bem compreendida se a organização identificar corretamente os riscos emergentes e usar as informações sobre ameaças obtidas interna ou externamente;

- **Passo 5: Criação do Perfil Alvo** – este Perfil é criado com base na avaliação das Categorias e Subcategorias já identificadas, onde estão descritos os resultados de cibersegurança que são desejados pela organização. As organizações também têm liberdade para definir as suas próprias Categorias e Subcategorias de forma a incluir todos os riscos organizacionais. Entidades do setor, clientes e parceiros de negócios da organização também podem ser ponderados pela mesma para a criação deste Perfil. Por fim, o Perfil Alvo deve refletir apropriadamente os critérios para o *Tier* alvo;
- **Passo 6: Determinar, analisar e prioritizar falhas** – Os Perfis anteriormente definidos são comparados de forma a detetar falhas. Com base na missão, custos, benefícios e riscos, a organização deve criar um plano de ação de combate a essas falhas de forma a atingir o Perfil Alvo. O plano de ação deve incluir os recursos necessários para o combate a estas falhas, incluindo financiamento e colaboradores. Os Perfis vão incentivar a organização a tomar decisões informadas sobre as atividades de cibersegurança, apoiar a gestão dos riscos e permitir que possam executar melhorias direcionadas e económicas; e
- **Passo 7: Implementar o Plano de Ação** – a organização deve determinar quais as ações a tomar para resolver as falhas identificadas no passo anterior e, logo de seguida, adaptar as suas práticas atuais de cibersegurança para atingir o seu Perfil Alvo.

3 Cronograma

Ao longo deste capítulo serão indicadas as tarefas executadas durante todo o projeto, o tempo de execução das mesmas e o Gráfico de *Gantt* como demonstração do intervalo temporal.

3.1 Tarefas

Este projeto passará por diferentes fases ao longo de todo o ano letivo. Começa pela realização do estudo do tema, isto é:

- Planeamento inicial do contexto, da motivação e dos objetivos do trabalho;
- Estudo das tecnologias e trabalhos relacionados.

Após esta parte, passa-se para a plataforma de configurações. O planeamento e a idealização são os principais pontos:

- Planeamento:
  - Estudo dos equipamentos;
  - Estruturação da Plataforma;
  - Diagramas;
  - *Mockups*;
  - Funcionamento.

A segunda fase do projeto passa pela implementação da *Smart Room*, tendo em conta os seguintes pontos:

- Planeamento:
  - Escolha dos sensores a implementar;
  - Aquisição dos sensores a aplicar e equipamentos acessórios;
  - Estruturação dos serviços e plataforma de apresentação dos dados;
  - Planeamento da arquitetura a implementar.
- Implementação:
  - Instalação e configuração dos diferentes sensores;

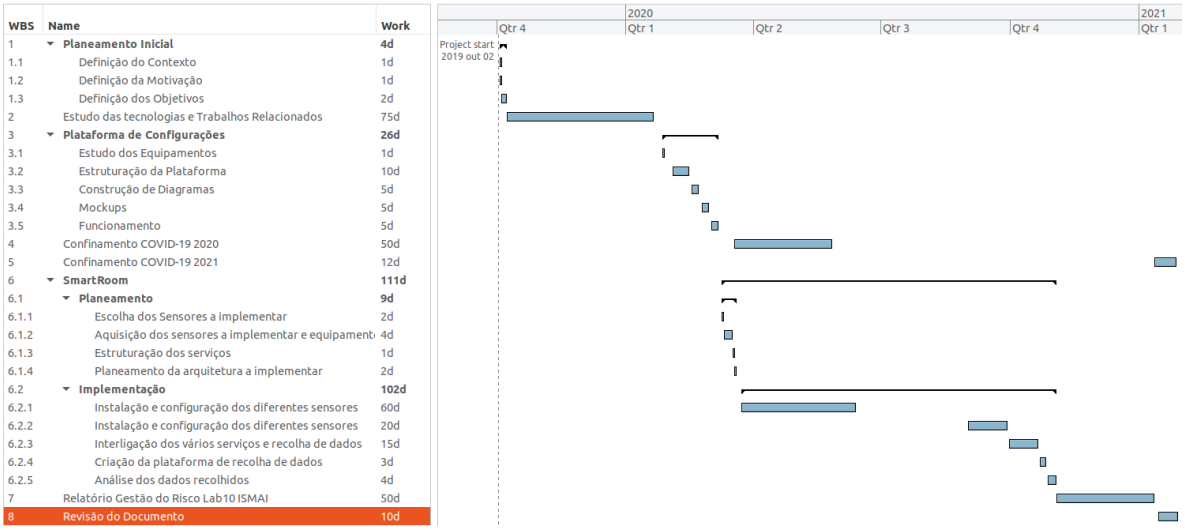
- Interligação com os vários serviços e recolha de dados;
- Criação da plataforma de recolha de dados;
- Análise dos dados recolhidos.

Por fim, e não menos importante, a criação do Relatório de Gestão do Risco do Laboratório de Redes e Sistemas Informáticos do ISMAI.

WBS	Name	Work
1	**Planeamento Inicial**	**4d**
1.1	Definição do Contexto	1d
1.2	Definição da Motivação	1d
1.3	Definição dos Objetivos	2d
2	Estudo das tecnologias e Trabalhos Relacionados	75d
3	**Plataforma de Configurações**	**26d**
3.1	Estudo dos Equipamentos	1d
3.2	Estruturação da Plataforma	10d
3.3	Construção de Diagramas	5d
3.4	Mockups	5d
3.5	Funcionamento	5d
4	Confinamento COVID-19 2020	50d
5	Confinamento COVID-19 2021	12d
6	**SmartRoom**	**111d**
6.1	**Planeamento**	**9d**
6.1.1	Escolha dos Sensores a implementar	2d
6.1.2	Aquisição dos sensores a implementar e equipament	4d
6.1.3	Estruturação dos serviços	1d
6.1.4	Planeamento da arquitetura a implementar	2d
6.2	**Implementação**	**102d**
6.2.1	Instalação e configuração dos diferentes sensores	60d
6.2.2	Instalação e configuração dos diferentes sensores	20d
6.2.3	Interligação dos vários serviços e recolha de dados	15d
6.2.4	Criação da plataforma de recolha de dados	3d
6.2.5	Análise dos dados recolhidos	4d
7	Relatório Gestão do Risco Lab10 ISMAI	50d
8	Revisão do Documento	10d

Figura 15 - Tarefas

3.2 Gráfico de Gantt



WBS	Name	Work
1	**Planeamento Inicial**	**4d**
1.1	Definição do Contexto	1d
1.2	Definição da Motivação	1d
1.3	Definição dos Objetivos	2d
2	Estudo das tecnologias e Trabalhos Relacionados	75d
3	**Plataforma de Configurações**	**26d**
3.1	Estudo dos Equipamentos	1d
3.2	Estruturação da Plataforma	10d
3.3	Construção de Diagramas	5d
3.4	Mockups	5d
3.5	Funcionamento	5d
4	Confinamento COVID-19 2020	50d
5	Confinamento COVID-19 2021	12d
6	**SmartRoom**	**111d**
6.1	**Planeamento**	**9d**
6.1.1	Escolha dos Sensores a implementar	2d
6.1.2	Aquisição dos sensores a implementar e equipament	4d
6.1.3	Estruturação dos serviços	1d
6.1.4	Planeamento da arquitetura a implementar	2d
6.2	**Implementação**	**102d**
6.2.1	Instalação e configuração dos diferentes sensores	60d
6.2.2	Instalação e configuração dos diferentes sensores	20d
6.2.3	Interligação dos vários serviços e recolha de dados	15d
6.2.4	Criação da plataforma de recolha de dados	3d
6.2.5	Análise dos dados recolhidos	4d
7	Relatório Gestão do Risco Lab10 ISMAI	50d
8	Revisão do Documento	10d

Figura 16 – Gráfico de Gantt

4 Implementação

Neste capítulo será explicada a implementação de cada um dos objetivos. Por cada objetivo será descrito, de forma respetiva, o que foi necessário para essa mesma implementação e como funciona.

4.1 Plataforma

A plataforma descrita ao longo deste capítulo tem como objetivo permitir que os docentes possam fazer o *download* e *upload* das configurações dos equipamentos presentes no laboratório 10 destinado às disciplinas lecionadas no laboratório 10. Esta plataforma foi pensada de forma a melhorar o processo atual existente de preparação e término das aulas e testes práticos.

A plataforma foi pensada para ser implementada numa máquina com o sistema operativo *Linux.* A escolha do sistema operativo em questão baseou-se no facto de o mesmo ser *open-source*, gratuito, flexível, seguro, de uso comum e aconselhado para a utilização tanto de PHP como de MySQL. O sistema de gestão de base de dados (SGBD) deverá ser *MySQL*, com a estrutura descrita no modelo relacional apresentado posteriormente. A escolha deste SGBD teve origem no facto de já haver familiaridade anterior.

A plataforma, tal como descrito nos pontos seguintes, é constituída por quatro páginas: *Login*, Ficheiros, *Download* e *Upload*.

4.1.1 Diagramas

Os diagramas apresentados neste capítulo vão permitir uma melhor compreensão do possível funcionamento da plataforma e de que forma cada uma das atividades é executada dentro do próprio sistema. Nos próximos pontos serão apresentados um diagrama de classes, um diagrama de casos de uso e quatro diagramas de atividades.

4.1.1.1 Diagrama de Classes

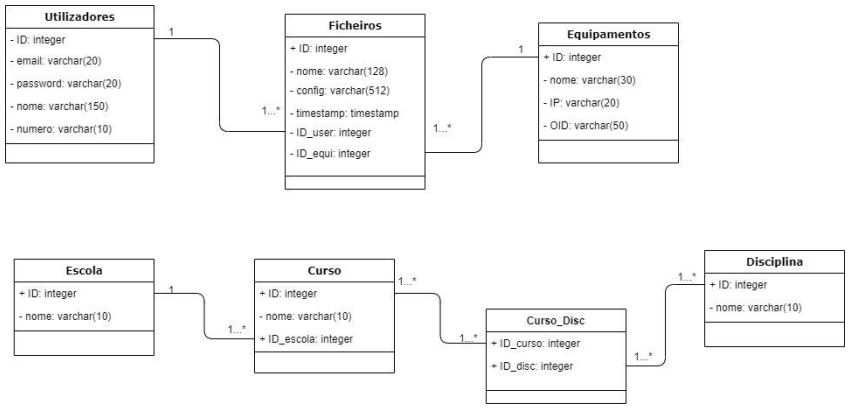


Figura 17 – Diagrama de Classes

O diagrama de classes foi feito no *software* online Draw.io (*Diagrams.Net*, n.d.). Segundo Guedes, 2018, um diagrama de classes "*apresenta uma visão estática de como as classes estão organizadas*", permitindo a compreensão do sistema com base nos atributos e métodos necessários.

O diagrama da Figura 17 permite-nos determinar que:

- Um ou mais utilizadores poderão ter a si associado um ou mais ficheiros;
- Cada ficheiro tem associado um e só um utilizador;
- Um ficheiro tem associado um e só um equipamento;
- Um equipamento poderá estar associado a um ou mais ficheiros;
- Uma escola tem associados um ou mais cursos;
- Um curso está associado a uma e só uma escola;
- Um curso está associado a uma ou mais disciplinas; e
- Uma disciplina está associada a um ou mais cursos.

4.1.1.2 Diagrama de Casos de Uso

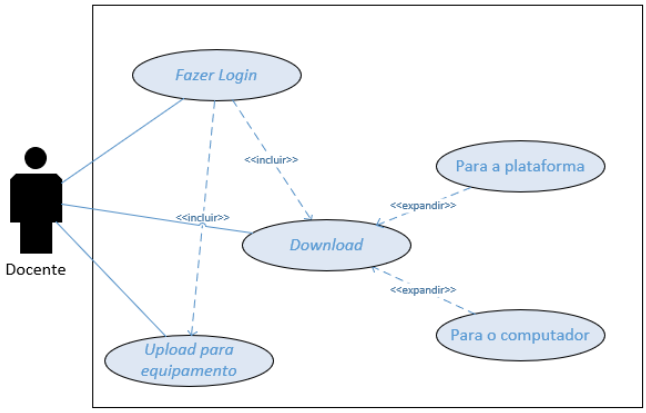


Figura 18 – Diagrama de Casos de Uso

Segundo Guedes, 2018, um digrama de casos de uso vai permitir associar tarefas ou funcionalidades essenciais ao funcionamento de um *software* à pessoa/sistema que pode executar essas mesmas tarefas.

No diagrama de casos de uso criado para esta plataforma, o ator é identificado como o docente, sendo que é ele que executará as ações na plataforma. As ações poderão ser *login*, *download* e *upload*.

As últimas duas estão incluídas no "*login*" pois só podem ser executadas após o utilizador iniciar sessão na plataforma. O *download* pode ser expandido para duas atividades, isto é, permitirá o *download* para a plataforma ou para o computador que está a ser utilizado para aceder à plataforma.

4.1.1.3 Diagrama de Atividades – Login

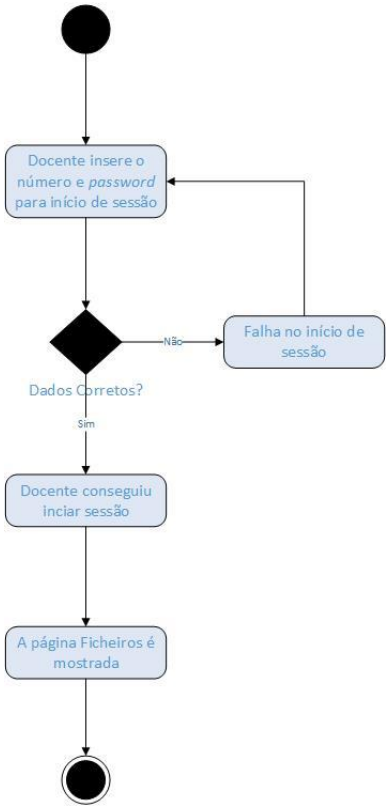


Figura 19 – Diagrama de Atividades – Login

O diagrama de atividades permite a descrição de uma atividade, em específico, executada na plataforma. A atividade apenas se poderá iniciar se o utilizador efetuar *login* na plataforma. Esse *login* começará pelo utilizador a inserir os seus dados na plataforma (número e *password*). Se os dados estiverem errados, o utilizador terá de os inserir novamente. Se estiverem corretos, a atividade prosseguirá. Quando o utilizador efetuar o início de sessão aparecerá a página "Ficheiros".

4.1.1.4 Diagrama de Atividades – Download

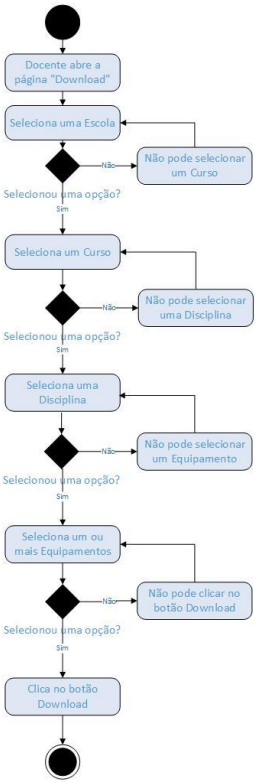


Figura 20 – Diagrama de Atividades – Download

O diagrama apresentado na Figura 20 exemplifica como decorre o *download*. O processo começa por o utilizador aceder à página "*Download*". Após isso, o utilizador tem de selecionar uma escola, obrigatoriamente, senão não pode selecionar um curso e assim sucessivamente até escolher um ou mais equipamentos. O utilizador só conseguirá clicar no botão "*Download*" se selecionar todas as opções: Escola, Curso, Disciplina e Equipamento(s).

4.1.1.5 Diagrama de Atividades – Upload

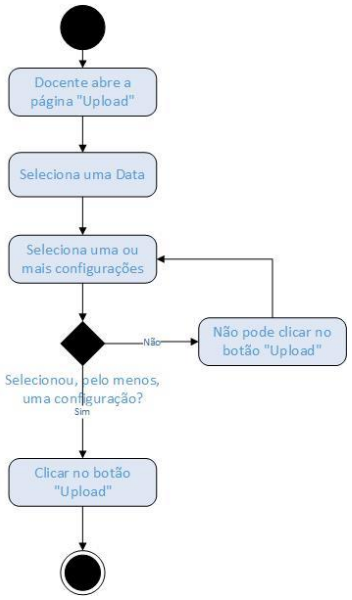


Figura 21 – Diagrama de Atividades – Upload

O diagrama de atividades de *Upload* explica que o utilizador tem de aceder à página *Upload*, selecionar a data de quando fez o *download* do ficheiro, selecionar obrigatoriamente um ou mais ficheiros e só com isso poderá selecionar o botão "*Upload*".

4.1.1.6 Diagrama de Atividades - Ficheiros

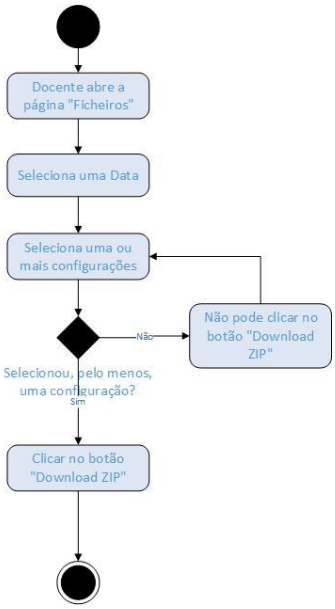


Figura 22 – Diagrama de Atividades – Ficheiros

O diagrama de atividades da página "Ficheiros" demonstra que o utilizador, ao aceder a esta página, pode verificar quais as configurações a que fez *download* anteriormente, estando organizadas por data. Esta página também permite, ao selecionar a data, selecionar uma ou mais configurações para fazer um *download* em ZIP para o computador em que acede à plataforma.

4.1.2 Mockups

Os *mockups* foram criados para representar o possível design da plataforma. Foram apresentados *mockups* de cada uma das páginas e quais os possíveis casos em cada uma delas. O seu funcionamento será explicado juntamente com a página em questão, nos pontos seguintes.

Para a identificação dos equipamentos foram escolhidas as seguintes siglas:

- RN – Router Nokia;
- RCB – Router Cisco Bastidor B;
- RCC – Router Cisco Bastidor C;
- FB – Firewall Bastidor B;
- FC – Firewall Bastidos C;
- SCB – Switch Cisco Bastidor B; e
- SCC – Switch Cisco Bastidor C.

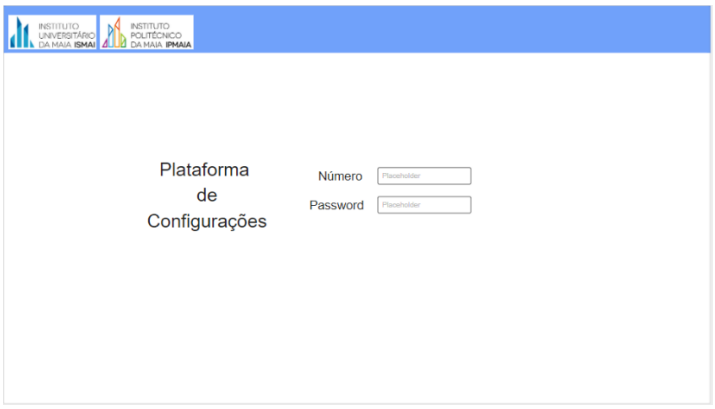


Figura 23 – *Mockup* da página *Login*

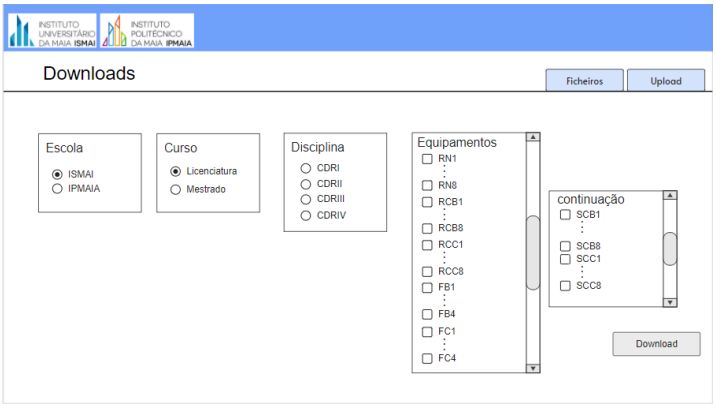


Figura 24 – *Mockup* da página *Downloads* (ISMAI-LIC)

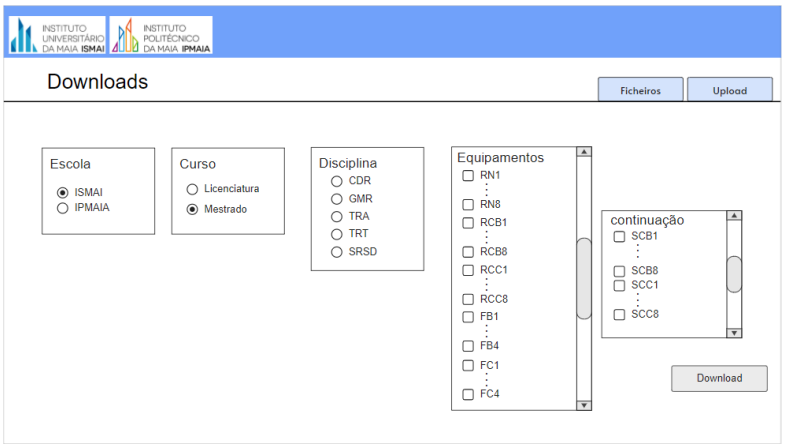


Figura 25 - *Mockup* da página *Downloads* (ISMAI-MES)

Nas Figuras 24 e 25 estão representados dois exemplos de seleções possíveis para a escola ISMAI. Na primeira figura é selecionada a escola ISMAI e o curso Licenciatura e, na segunda figura, o curso Mestrado. É importante salientar que as Disciplinas variam por Curso e, portanto, foram descritos os dois exemplos para demonstrar o dinamismo pretendido na plataforma.

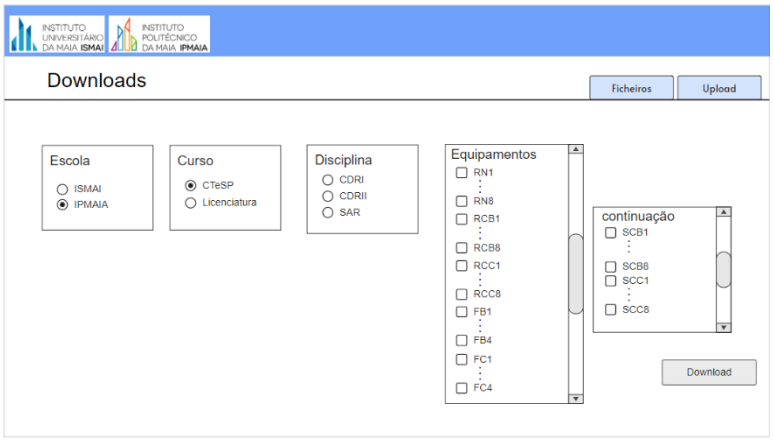


Figura 26 - *Mockup* da página *Downloads* (IPMAIA-CT)

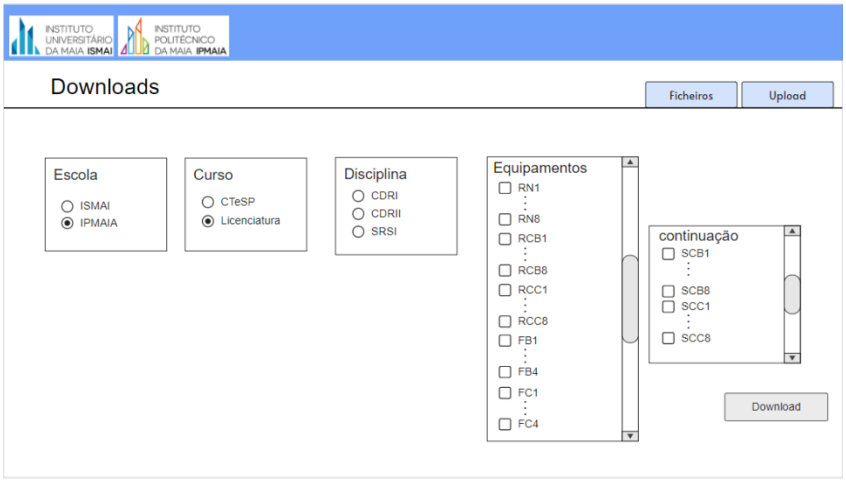


Figura 27 - *Mockup* da página *Downloads* (IPMAIA-LIC)

Nas Figuras 26 e 27 apresenta-se exemplos de caminhos com a Escola IPMAIA. Ao ser selecionada a escola IPMAIA, poderá selecionar-se o curso "CTeSP" ou o curso "Licenciatura" e, para cada curso, aparecem as disciplinas respetivas.

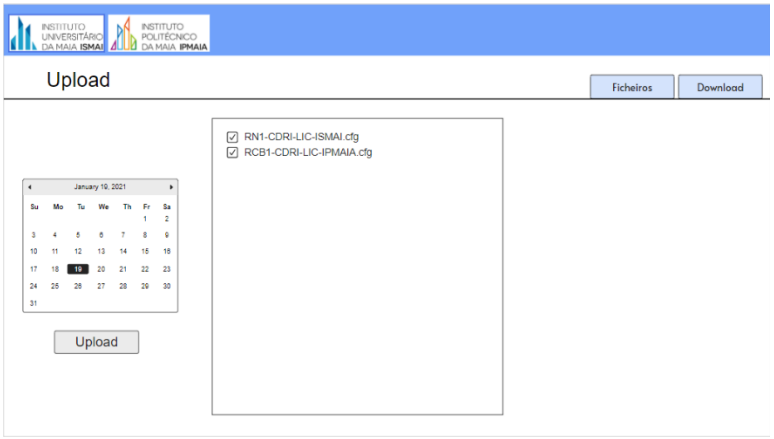


Figura 28 - *Mockup* da página *Uploads*

Na Figura 28 temos a representação do *layout* da página "*Upload*". O utilizador, ao selecionar uma data, poderá consultar as configurações que foram guardadas na Plataforma na data em questão. Se o utilizador pretender fazer o *upload* de uma ou mais configurações, o mesmo terá de selecionar as configurações pretendidas e carregar no botão *Upload*.

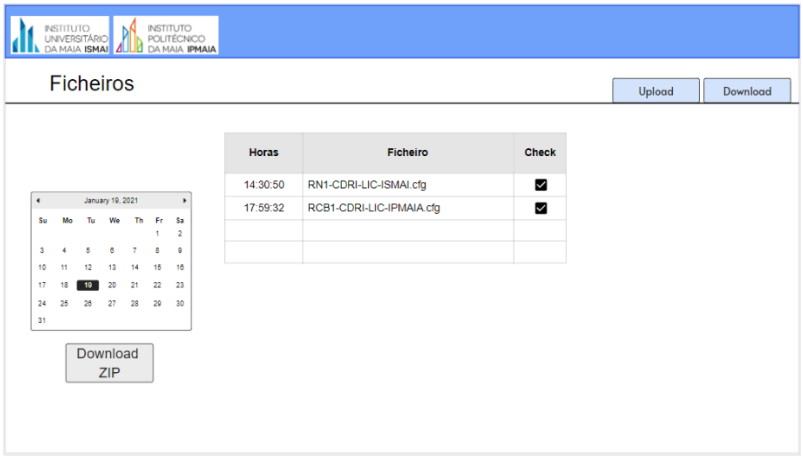


Figura 29 - *Mockup* da página Ficheiros

A página "Ficheiros" é apresentada quando o utilizador inicia sessão e também pode ser acedida através do menu do lado direito, em cima. Esta página permitirá aos utilizadores, conforme a data que selecionarem, fazerem o download em formato *ZIP* das configurações para o computador a partir do qual estão a aceder à plataforma.

4.1.3 Funcionamento

4.1.3.1 Downloads

Os equipamentos que devem ser abrangidos por esta plataforma são *routers* Nokia e *routers*, *switch* e *firewall* CISCO (todos já instalados no Laboratório 10). Esta informação foi selecionada da lista de equipamentos também fornecida no questionário apresentado no Anexo 12.

As opções selecionadas pelo utilizador, nomeadamente, a Escola, o Curso, a Disciplina e o Equipamento, devem ser armazenadas temporariamente pela plataforma para serem utilizadas na construção do nome do ficheiro de configuração daquele equipamento.

Após o utilizador clicar no botão "*Download*", o programa executará um *script* que fará o tratamento dos dados recolhidos anteriormente. Essa informação vai ser importante

para saber qual o IP do equipamento em que é preciso recolher a configuração e construir o nome que será dado ao ficheiro de configuração.

A ligação ao equipamento deverá ser feita por SSH. Nesta ligação é importante indicar qual o IP do equipamento de destino e quais os dados de administração do equipamento, para que a autenticação seja automatizável.

O ficheiro de configuração deve ser recolhido com o uso do protocolo SCP e guardado numa pasta do servidor, em que o nome do ficheiro é construído com base no caminho escolhido nas *radiobutton*. Após ser guardado localmente, é possível enviá-lo para a base de dados, mantendo assim o ficheiro acessível a outras funcionalidades disponíveis na plataforma.

4.1.3.2 Uploads

O utilizador poderá usufruir desta funcionalidade da plataforma sempre que necessitar de enviar uma configuração para um equipamento. Após selecionar a ou as configurações, a plataforma executará um *script*. Este precisará de requisitar à base de dados a informação necessária para este processo: IP para a conexão e o OID para a execução do da instrução SNMP para *reboot* do equipamento.

A conexão ao equipamento deve ser feita por SSH. E, tal como no ponto anterior, a conexão deve utilizar o IP do equipamento e a descrição dos dados de autenticação no equipamento. A configuração em questão deve ser retirada da base de dados e o caminho de destino desse ficheiro deve ser descrito nos comandos SCP necessários para a inserção da configuração no equipamento.

Para os equipamentos Nokia é preciso ter em consideração que os mesmos necessitam de ser reiniciados após o carregamento de uma nova configuração. Para isso, deverá ser utilizado o protocolo SNMP. Este serviço deverá estar disponível quer no servidor quer no equipamento.

4.1.3.3 Download ZIP

O principal objetivo da plataforma, para além de facilitar os processos descritos anteriormente, é também permitir que as configurações fiquem guardadas de forma a poderem ser acedidas sempre que os docentes necessitem. Mas, devido ao funcionamento do laboratório, também é importante poderem partilhar esses ficheiros e, para isso, na página "Ficheiros" haverá um botão que permitirá ao utilizador fazer um *download* em formato ZIP com todas as configurações que necessitar.

A plataforma deverá permitir que seja selecionada a data em que o utilizador efetuou o *download* do ficheiro do equipamento e o utilizador terá de selecionar um ou mais ficheiros daquela data. Com esta ação, será possível o utilizador clicar no botão "*Download* ZIP" e, aí, o programa terá de colocar o nome desse ZIP com a data que foi selecionada pelo utilizador na sua filtragem da seleção de ficheiros. Esta data poderá ser conseguida através da consulta da base de dados, na tabela ficheiros.

4.2 *SmartRoom* – Sensores

A utilização de sensores num determinado espaço tem o objetivo de fazer um controlo inteligente do espaço em questão. Esse controlo inteligente é permitido através do uso de diferentes *hardware, software*, linguagens e implementações. Os sensores selecionados para a sala técnica do laboratório 10 vão ser explicados ao longo deste capítulo.

4.2.1 Hardware

4.2.1.1 Fonte de alimentação

Figura 30 – Power Supply (*Breadboard Power Supply Module 3.3V/5V*, n.d.)

Na Figura 30 retrata-se o módulo de fonte de alimentação para a *breadboard* (fonte DC-DC) com saídas de 3.3V e 5V e com uma entrada de 6.5V até 12V. Também pode ser utilizado através da porta USB.

Segundo a Handsontec, 2017, as principais características deste componente são:

- Intervalos de tensão de entrada: DC 6.5V a 12V ou DC 5V da porta USB;
- Tensões de saída: 3.3V e 5V, com opção de escolha usando *jumpers*;
- Máximo de corrente de saída: <700mA;
- Botão ON/OFF.

4.2.1.2 Transformador

Figura 31 – Transformador 30W (*FE & MO TECHNOLOGY S.L.U*, n.d.)

Na Figura 31 apresenta-se o transformador adotado para a criação dos módulos discutidos durante este capítulo. De salientar que o facto de ser regulável disponibiliza uma maior versatilidade. Para o trabalho em questão foi mantido em 7.5V, tensão que se considerou ser a mais adequada dado que a fonte DC-DC necessita de ser alimentada com uma tensão mínima de 6.5V e a tensão mais próxima disponibilizada por este transformador que seja igual ou superior a 6.5V é de 7V. As características do equipamento utilizado são (*FE & MO TECHNOLOGY S.L.U*, n.d.):

- "*Tensão de entrada – AC 100V a 240V;*
- *Corrente de entrada – 1.0A;*
- *Tensões de saída – DC 3V/4.5V/5V/6V/7.5V/9V/12V;*
- *Corrente de saída - 2.0A máximo;*
- *1 porta USB – 5V/1.2A*".

4.2.1.3 Arduino Nano

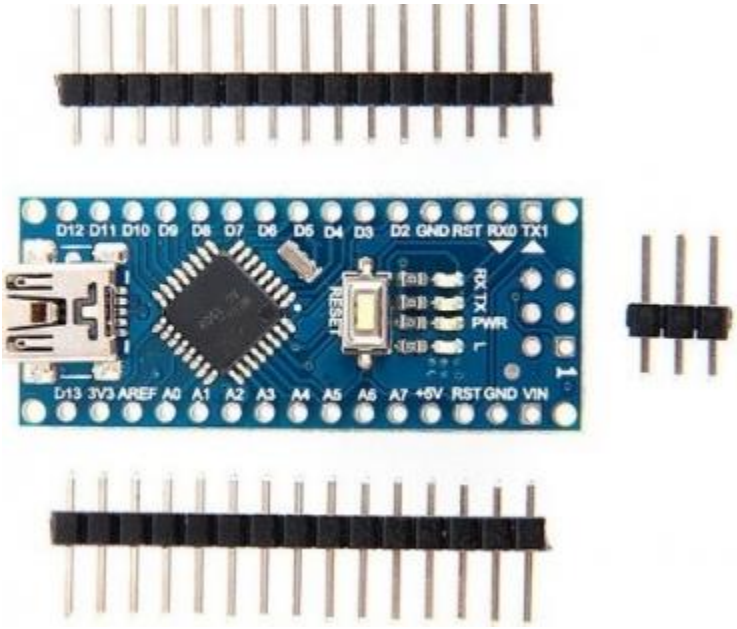


Figura 32 – Arduino Nano (*Arduino Nano | Arduino Official Store*, n.d.)

O Arduino Nano é um Arduino pequeno, simples e compacto que permite a sua utilização direta com a *breadboard*. Segundo a loja oficial da marca, as suas características são:

- Microcontrolador – Atmega328;
- Tensão de operação – 5V;
- Memória *flash* – 32KB sendo que 2KB são para o *bootloader*;
- Portas Digitais – 12 portas sendo que seis são PWM;
- Portas Analógicas – 8 portas;
- Velocidade do Relógio – 16 MHz;
- Tensão de entrada – 7V a 12V;
- Consumo de Energia - 19mA;

4.2.1.4 Placa de Rede

Figura 33 – Placa de Rede ENC28J60

Segundo a Microchip Technology Inc., 2006, as principais características deste componente são:

- Controlador Ethernet: IEEE 802.3;
- Compatibilidade de Rede: 10/100/1000BASE-T, de salientar que a placa de rede não funciona a mais de 10Mbps;
- Tensão de Operação: 3.1V a 3.6V, preferivelmente 3.3V;
- Intervalo de temperatura de operação: versão industrial de -40ºC a +85ºC e versão comercial de 0ºC a +70ºC;
- Conexão com o microcontrolador: SPI.

As ligações desta placa de rede são comuns a todos os módulos e são as seguintes:

1	2
RST – RST	VCC – 3.3V
INT – D8	GND – GND
	MISO – D12
	MOSI – D11
	SCK – D13
	CS – D10

De salientar que, em todos os módulos, o VCC ficou diretamente ligado à fonte de alimentação, garantindo que a *breadboard* não interferisse causando instabilidade.

4.2.1.5 Breadboard

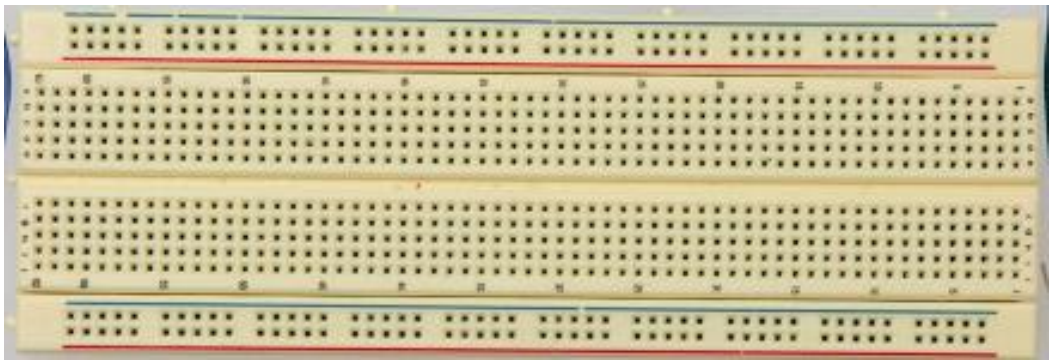


Figura 34 – Breadboard (*Arduino - Setting up an Arduino on a Breadboard*, n.d.)

As duas linhas exteriores marcadas a azul e a vermelho, respetivamente, por convenção são utilizadas para alimentação. As linhas vermelhas correspondem ao positivo (+) e as linhas azuis correspondem ao negativo (-). Neste modelo da *breadboard*, cada uma dessas duas linhas conecta a totalidade dos pontos respetivos.

No centro da *breadboard*, as colunas são definidas por dois grupos de letras [a,b,c,d,e] e [f,g,h,i,j] e existem marcações de cinco em cinco linhas. A conexão feita nesta área é na vertical (em relação à orientação da Figura 34), isto é, na primeira coluna, todos os espaços na linha do número 1 estão ligados entre si, o mesmo acontecendo nas restantes.

4.2.1.6 Sensor DHT11

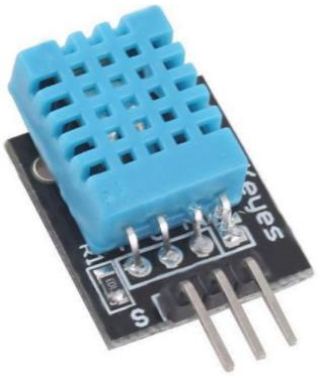


Figura 35 – Sensor DHT11 (*DHT11 Sensor Pinout, Features, Equivalents & Datasheet*, n.d.)

O sensor DHT11 é um sensor com capacidade de medição da temperatura e humidade de um determinado local. Segundo a Aosong Electronics, 2010 as especificações dele são as seguintes:

- Tensão de operação: 3.5V a 5.5V;
- Corrente de operação: 0.3mA (em medição) 60uA (*standby*);
- *Output*: *Serial data*;
- Intervalo de Temperatura: de 0°C a 50°C;
- Intervalo de Humidade: de 20% a 90%;
- Precisão: ±1°C e ±1%.

4.2.1.7 Sensor de som

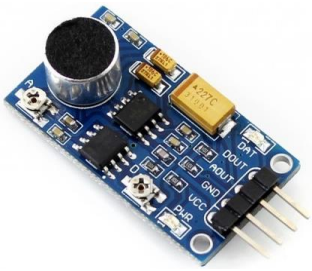


Figura 36 – Sensor de Som Waveshare 9534 (*Sensor de Som c/ Saída Analógica e Digital*, n.d.)

O sensor de som utilizado neste projeto foi o modelo 9534 da Waveshare, baseado no amplificador LM386, que permite a leitura de dados por vias analógica e digital. As especificações deste modelo são as seguintes:

- Sensibilidade do microfone: 52dB;
- Intervalo de frequência: 50Hz a 20KHz;
- Tensão de operação: de 3.3V a 5.3V.

4.2.1.8 Sensor de gás

Figura 37 – Sensor de Gases MQ-135 (*Sensor de Gases MQ-135*, n.d.)

Este sensor de gás permite controlar a qualidade do ar no local onde é colocado. Segundo Olimex, 2013, este modelo permite a deteção de gases NH_3 (amoníaco), NO_x (óxidos de nitrogénio), álcool, benzeno, fumo, CO_2 (dióxido de carbono), entre outros. Segundo o mesmo autor, as principais características deste componente são:

- Tensão de operação: 5V;
- Tensão de aquecimento: 5V;
- Resistência de carregamento: ajustável;
- Resistência de calor: 33Ω;
- Resistência de deteção: de 30KΩ a 200KΩ.

4.2.1.9 Sensor nível de água

Figura 38 – Sensor de Nível de Água VMA303 (*VMA303: MÓDULO DE SENSOR DE HUMIDADE DO SOLO & SENSOR DE NÍVEL DE ÁGUA – Velleman – Wholesaler and Developer of Electronics*, n.d.)

Segundo o fabricante, este sensor é utilizado para medir o nível de água até 4cm. A medição poderá ser analógica ou digital. A tensão com que trabalha é de 5V.

4.2.1.10 RFID

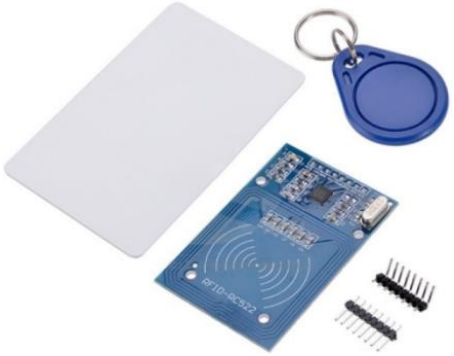


Figura 39 – Módulo Leitor RFID RC522 (*Módulo Leitor RFID RC522 Arduino*, n.d.)

O módulo representado na Figura 39 é baseado no circuito integrado MFRC-522. Este sensor suporta leitura e escrita *Mifare* e comunica por SPI, I2C ou UART com o microcontrolador. Segundo Keeler, 2004, as especificações deste sensor são:

- "*Frequência da Comunicação: 13,56MHz;*
- *Consumo: 13-25mA a 3.3V;*
- *Tipos de cartões suportados: Mifare1 S50, S70 Mifare1, Mifare UltraLight, Mifare Pro, Mifare Desfire;*
- *Temperatura Operacional: de -20ºC a 80ºC;*
- *Temperatura de armazenamento: de -40ºC a 85ºC;*
- *Taxa de transferência: 10 Mbit/s.*"

4.2.1.11 LCD

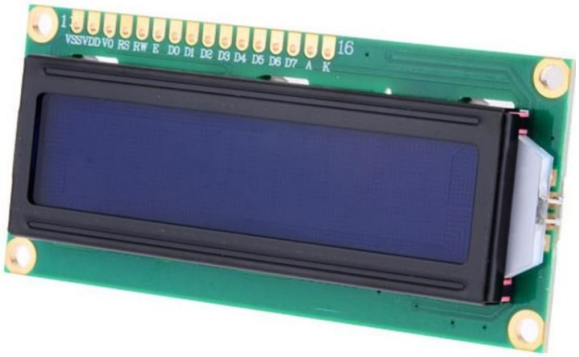


Figura 40 – Display LCD 16x2 (*Display LCD 16x2 I2C Com Fundo Azul*, n.d.)

Este LCD é apenas de caracteres (sem suporte gráfico), constituído por 16 colunas e duas linhas, com luz de fundo azul e letras na cor branca. É compatível com diversos microcontroladores, incluindo o ATMega 328P em que o Arduino Nano utilizado neste projeto se baseia. Segundo a SHENZHEN RUITE ELECTRONIC CO., n.d., as especificações mais importantes são:

- Tensão de funcionamento: de 4.5V a 5.5V;
- Corrente de funcionamento: de 1.0mA a 1.5mA;
- Tensão do LED: de 1.5V a 5.5V;
- Corrente do LED: de 75mA a 200mA.

4.2.1.12 Conversor LCD

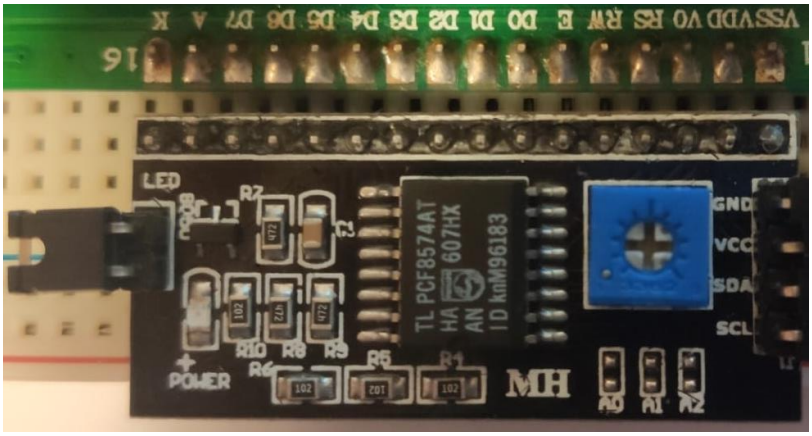


Figura 41 – Conversor Display LCD TL PCF8574AT

Este conversor tem 16 pinos que deverão estar alinhados com os 16 pinos do LCD, tal como está representado na Figura 41. Apesar de ser mais um componente a ocupar espaço na *breadboard*, tem a vantagem de reduzir a quantidade de ligações e, por conseguinte, de cabos que acabam por se cruzar com os restantes sensores do módulo. Adicionalmente, ajuda a prevenir a falha da conexão com o LCD, pois os cabos são frágeis e poderão não funcionar corretamente e, quando se usa uma *breadboard*, a probabilidade de maus contactos aumenta com o número de ligações. A *datasheet* apresentado pela Philips, 2002 apresenta todas as características necessárias para o conhecimento deste componente.

A ligação ao Arduino e à fonte de energia são feitas pelas seguintes portas:

I2C_LCD	ARDUINO
SDA	A4
SCL	A5
GND	GND
VCC	5V

4.2.1.13 PIR

Figura 42 – Sensor PIR (*Sensor PIR / Sensor Movimento Para Arduino*, n.d.)

O Sensor PIR apresentado na Figura acima é um sensor que deteta apenas movimento e não presença. Este sensor tem um alcance de até sete metros e um atraso programável na ativação do mesmo após detetar movimento, ambos regulados pelos potenciómetros representados na Figura 42. Segundo a Ada, 2020 as características deste componente são:

- Intervalo de tensão para funcionamento: DC 4.5V a 20V, recomendado o uso de 5V;
- Nível de saída: alto 3.3V e baixo 0V;
- Campo de visão: de 100º a 120º;
- Tempo de atraso: de 0.3s a 5min;
- Temperatura de operação: de -20 a +70ºC.

4.2.1.14 Relé

Figura 43 – Módulo de Relé de 5V (*1 Channel 5V Relay Shield Module*, n.d.)

O relé, em conjunto com o sensor PIR mencionado no ponto 4.2.1.13, vai permitir acionar uma lâmpada ou outro equipamento. Pode ser utilizado com diversos microcontroladores existentes no mercado incluindo o ATMega 328P que integra o Arduino.

No *borne* existem três conexões: NA (normalmente aberto), C (comum) e NF (normalmente fechado). A ligação terá de ser feita sempre entre NA-C ou C-NF. NA-C é utilizado quando queremos que o relé permaneça aberto, isto é, o circuito esteja interrompido e apenas mude o estado quando há um sinal para fechar este circuito (a lâmpada começa desligada e só liga quando há um sinal transmitido). C-NF acontece o inverso, o circuito está fechado e apenas é interrompido quando há um sinal a indicar o contrário (a lâmpada começa ligada e apenas desliga quando indicado).

Este componente utiliza uma tensão de operação de 5V e dá para trabalhar com cargas até 220V AC.

4.2.2 Software e Linguagem

A análise dos dados recolhidos pelos módulos apenas é possível com recurso a determinado *software* e linguagens que permitam a configuração dos Arduinos, a conexão à base de dados e a inserção dos valores recolhidos na base de dados.

4.2.2.1 Arduino IDE

Este *software* tem como principal objetivo facilitar a construção, em linguagem C++, do código necessário para o funcionamento das placas Arduino e a sua comunicação com os sensores. A utilização é bastante intuitiva e simples, mas é importante ter alguns pontos em conta na primeira vez que se utiliza o mesmo.

Após a abertura do programa é necessário dar a conhecer ao mesmo quais as características dos componentes com que ele vai trabalhar e onde ele pode aceder aos mesmos. No caso do projeto implementado as características selecionadas foram as descritas na Figura 44.

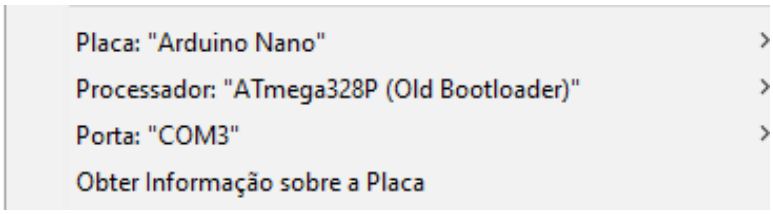


Figura 44 – Arduino IDE – menu Ferramentas

Outra funcionalidade deste *software* é ter disponível bibliotecas que facilitam a inicialização e manipulação de diversos componentes. Estão disponíveis para instalação diversas bibliotecas diretamente a partir do IDE, mas também aceita a adição de bibliotecas externas.

No projeto em causa apenas uma das bibliotecas utilizadas é comum a todos os módulos implementados. Essa biblioteca pertence à placa de rede apresentada no ponto 4.2.1.4 e chama-se *UIPEthernet.h*, sendo possível instalar diretamente a partir do Arduino IDE.

O *download* deste *software* pode ser feito aqui: https://www.arduino.cc/en/software.

4.2.2.2 PHP

O PHP é uma linguagem interpretada, cujo nome teve origem na expressão *Hypertext Preprocessor*.

A utilização de uma linguagem interpretada no *backend* permite que os *scripts* sejam facilmente atualizados sem necessidade de recompilação.

No projeto em causa, o PHP foi utilizado para fazer a conexão com a base de dados em MySQL, a inserção dos dados recolhidos nas tabelas e a apresentação desses resultados numa página.

Para cada tipo de valor recolhido pelos sensores criou-se uma página PHP. As páginas serão referenciadas juntamente com a explicação do módulo.

4.2.2.3 MySQL

O MySQL é um sistema de gestão de base de dados criado pela MySQL AB, adquirida mais tarde pela Sun Microsystems que, posteriormente, foi adquirida pela Oracle Corporation, e que suporta SQL como linguagem para manipulação dos dados. Por ser extremamente versátil, é utilizada pela maior parte dos programadores para desenvolver diversos tipos de plataformas e soluções de complexidade variada. É frequente o uso de MySQL em conjunto com a linguagem PHP. Para gerir bases de dados MySQL existem várias ferramentas, mas uma das mais comuns é a *phpMyAdmin*. Este interface é bastante intuitivo e simples, permitindo a criação da base de dados e das tabelas, tal como demonstra na Figura 45.

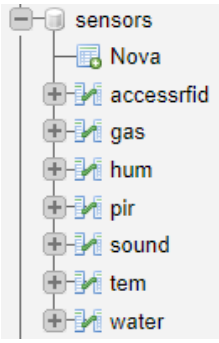


Figura 45 – Base de Dados e tabelas que constituem o projeto

4.2.3 Módulos de Implementação

4.2.3.1 Sensores de Som, Gás, DHT11 (Temperatura e Humidade)

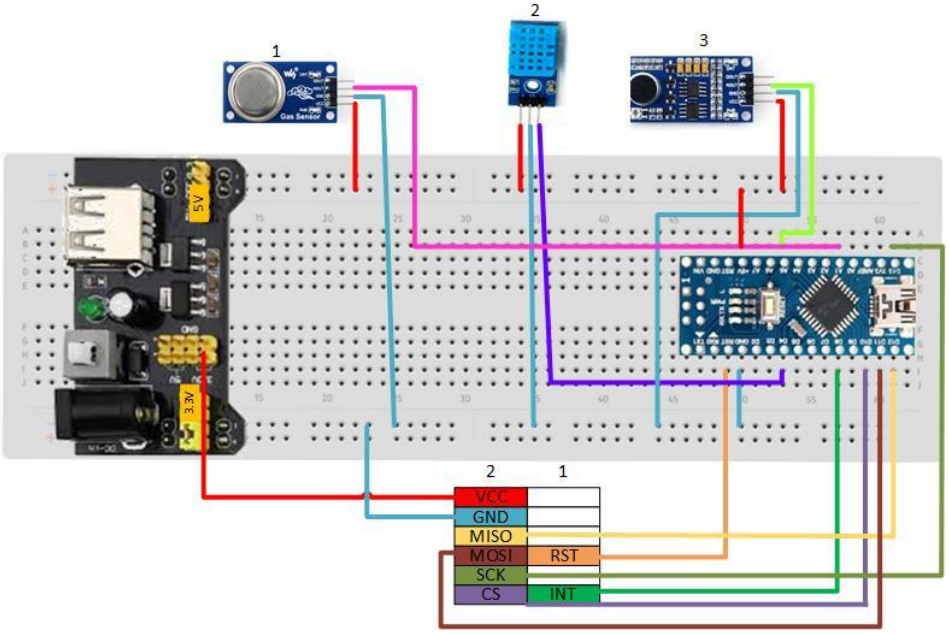


Figura 46 – Módulo de Sensores de Som, Gás, DHT11 (Temperatura e Humidade)

O módulo apresentado na Figura 46 representa as ligações necessárias para cada um dos sensores com o Arduino. O módulo, para além de ser constituído pelos sensores, também é constituído por uma placa de rede.

O sensor de gás (1) foi introduzido no ponto 4.2.1.8. É possível determinar, pelas ligações que para além da ligação positiva aos 5V e a negativa ao GND, os dados recolhidos pelo sensor serão de tipo analógico.

O sensor de humidade e temperatura (2), explicado no ponto 4.2.1.6, executa a leitura de temperatura em graus *Celsius* ou *Fahrenheit* e da humidade em percentagem. Neste projeto a temperatura foi lida apenas em graus *Celsius*.

Por fim, o sensor de som (3), introduzido no ponto 4.2.1.7, também permite leituras analógicas ou digitais. A leitura implementada neste módulo foi a analógica. A leitura digital por si só não tem sentido mas utilizada em conjunto com a leitura analógica permite que, por

exemplo, o sensor só efetue uma leitura analógica no caso de ser detetada a presença de som (leitura digital).

A placa de rede vai permitir enviar para o servidor os dados recolhidos pelos sensores, conforme definido no código do Arduino apresentado no Anexo1 (ponto 9.1). No servidor, os dados serão encaminhados para a base de dados através de um *script* PHP, cujo conteúdo é apresentado nos Anexos 5, 6, 7 e 8 (pontos 9.5, 9.6, 9.7 e 9.8).

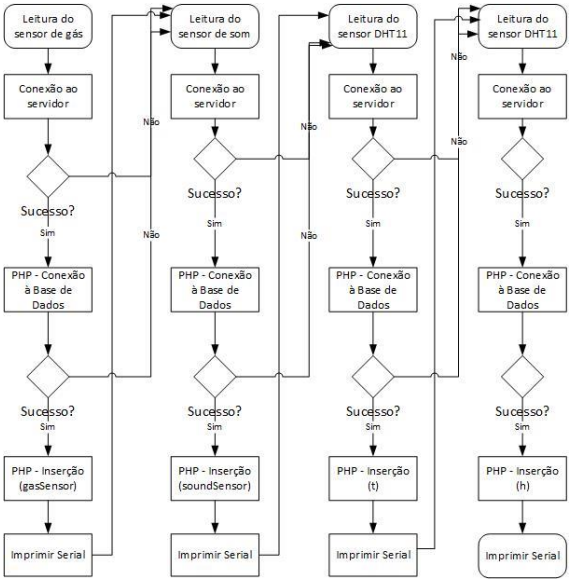


Figura 47 – Funcionamento Contínuo do Módulo de Sensores de Som, Gás, DHT11 (Temperatura e Humidade)

A Figura 47 representa o funcionamento do programa a partir do momento que entra na função *loop*. O código vai ser executado da esquerda para a direita, isto é, começa pelo sensor de gás, de seguida o som, temperatura e, por fim, humidade. Cada uma destas leituras é representada por funções que são executadas uma a seguir à outra e sempre com um intervalo de dois segundos entre elas. Este intervalo é importante para que toda a comunicação possa ser terminada.

No fim da leitura da humidade, o *loop* terá de esperar 10 minutos para fazer uma nova leitura

4.2.3.2 Sensor de Nível de Água

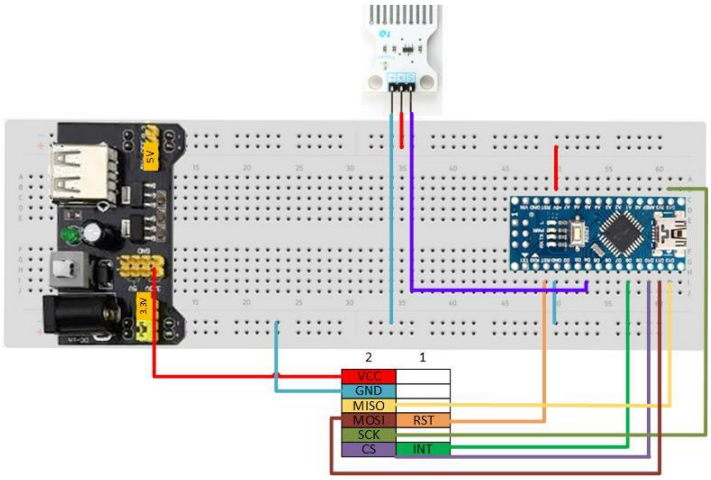


Figura 48 – Módulo de Sensor do Nível de Água

O módulo apresentado na Figura 48 é que contém o sensor de medição do nível da água. A leitura implementada neste módulo é digital porque o interesse é saber se existe água ou não no chão da sala técnica e não o nível dessa água.

O código do Arduino está no Anexo 2 (ponto 9.2) e o PHP, que fará a ligação à base de dados e a inserção dos valores na mesma está no Anexo 9 (ponto 9.9).

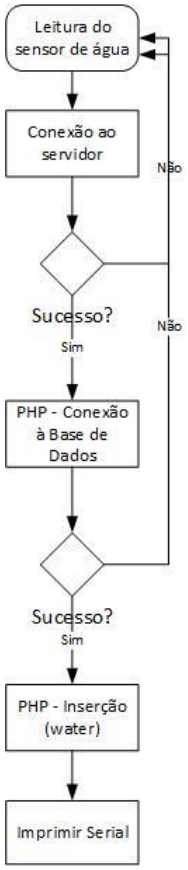


Figura 49 – Funcionamento Contínuo do Módulo de Sensor do Nível de Água

Na Figura 49, está demonstrado o funcionamento da função *loop* do Arduino.

4.2.3.3 Sensor de Movimento

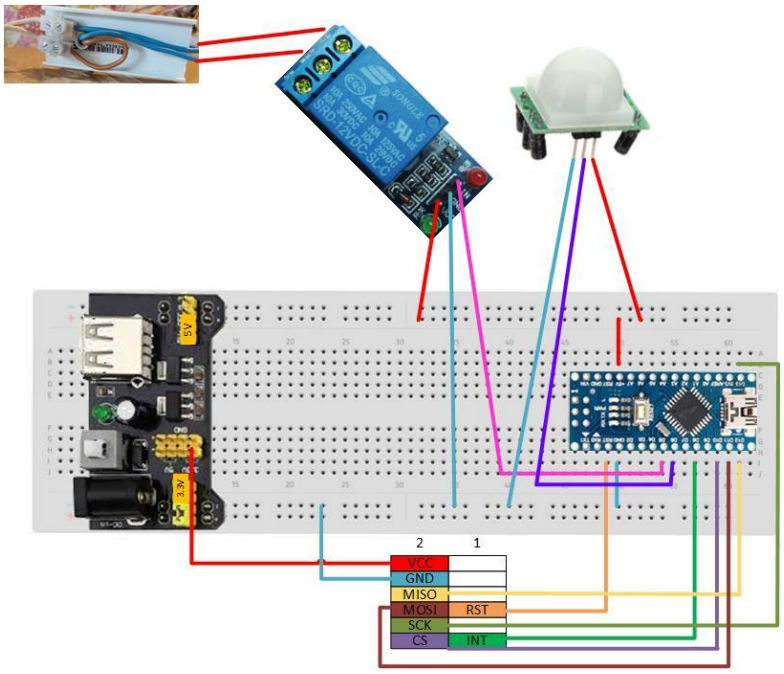


Figura 50 – Módulo com PIR e Relé

O módulo representado na Figura 50 tem a base dos outros módulos já apresentados, *breadboard*, Arduino e fonte de alimentação ligada a um transformador de 7,5V.

O sensor de movimento, à direita da imagem, tem a função de detetar movimento na sala técnica. A leitura do sensor será de tipo digital.

O relé permite controlar o acender ou apagar da lâmpada. Esse controlo é feito no código do módulo. A ligação da lâmpada ao relé foi feita pelo par NA-C, o que significa que a lâmpada começará desligada, tal como explicado no ponto 4.2.1.14 e só se acenderá se o sensor PIR detetar movimento.

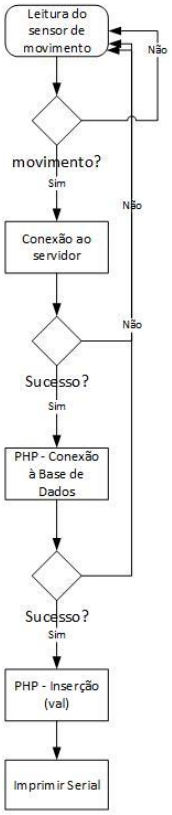


Figura 51 - Funcionamento Contínuo do Módulo de Sensor de Movimento

Na Figura 51 está representado o funcionamento do *loop* do programa. O mesmo apenas enviará dados para a base de dados quando detetar movimento, sendo importante que na tabela e na inserção à base de dados esteja o *timestamp*, sendo esse o campo que permitirá a distinção entre as diferentes inserções.

Os Anexos 3 e 10 (pontos 9.3 e 9.10) demonstram, respetivamente, os códigos do Arduino e o PHP utilizados.

4.2.3.4 Sensor RFID

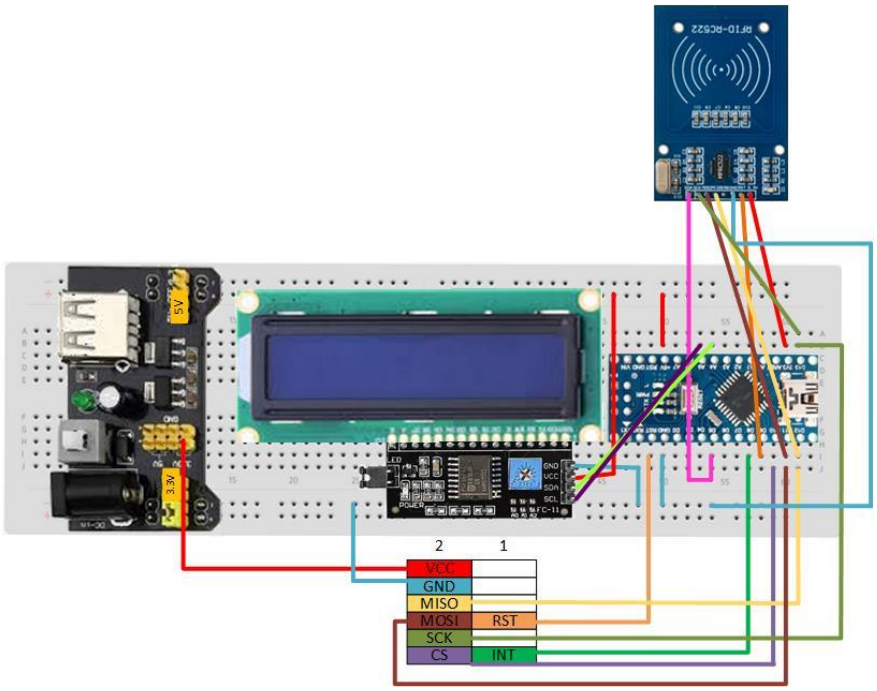


Figura 52 – Módulo de Controlo de Acesso

A Figura 52 representa a construção de um módulo de controlo de acesso com recurso ao RFID-RC522 e a um LCD, de forma a mostrar o nível autorização dado a uma determinada pessoa.

Para a conexão do LCD ao Arduino foi fundamental o uso de um conversor explicado no ponto 4.2.1.12.

O RFID lerá o UID do cartão ou pin que deverá ser previamente escrito no código. Se o UID tiver acesso, será mostrado no LCD “Bem Vindo/a!”. Logo de seguida será feita a conexão ao servidor e inserida na base de dados o UID do acesso autorizado.

No caso de o acesso não ser autorizado, apenas aparecerá uma mensagem no LCD a dizer “Acesso negado!".

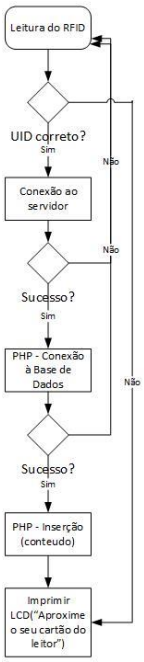


Figura 53 - Funcionamento Contínuo do Módulo de RFID

A Figura 53 apresenta o funcionamento da comunicação no módulo descrito neste capítulo. A informação é lida pelo sensor RFID e, de seguida, verifica-se se o UID lido faz parte da lista de UID ("`conteudo`") já registados. Se sim, o fluxo do código prossegue até à inserção na base de dados. Se não corresponder, mostra novamente a mensagem no LCD a indicar ao utilizador que pode fazer uma nova leitura.

Os Anexos 4 e 11 (pontos 9.4 e 9.11) demonstram, respetivamente, os códigos do Arduino e o PHP utilizados.

4.2.4 Plataforma de Sensores

A plataforma em questão foi criada com o objetivo de mostrar, de forma mais rápida e intuitiva, os dados guardados na base de dados criada para receber os valores recolhidos pelos sensores. A plataforma foi criada em PHP e utilizou-se a biblioteca *Bootstrap* para

fazer o design apresentado na Figura 54. Foi utilizada esta biblioteca devido à rapidez de implementação e a sua capacidade de tornar a plataforma responsiva.

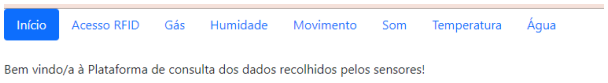


Figura 54 – Página *Home* da Plataforma de Sensores

As restantes páginas e o formato das mesmas estão descritos no ponto 5.2, onde serão apresentados os dados recolhidos dos sensores, nas Figuras 55 a 61.

4.3 Relatório de Gestão do Risco

A criação da nova sala técnica e a mudança de localização e tamanho do laboratório de redes e sistemas informáticos do ISMAI proporcionou um aumento de equipamentos, docentes e alunos a trabalhar com esse mesmo laboratório. Os aumentos mencionados ao longo de todo o relatório relativos ao melhoramento do laboratório 10 são diretamente proporcionais ao aumento do risco, das ameaças e vulnerabilidades do mesmo.

O Relatório de Gestão de Risco do Laboratório de Redes e Sistemas Informáticos do ISMAI (laboratório 10), presente no Anexo 13 (ponto 9.13), vai permitir, após uma pequena análise do que está atualmente implementado, perceber quais os cuidados a melhorar, tanto a nível de *hardware* como de *software*, para manter o laboratório 10 e toda a informação que lá circula seguros.

De forma a conhecer as ações implementadas a nível da gestão do risco e a opinião dos docentes e monitores do laboratório 10 relativamente à gestão do risco, elaborou-se um questionário de 17 perguntas. Este questionário foi enviado para os seis docentes e monitores do laboratório 10. As perguntas do questionário são apresentadas no Anexo 12 (ponto 9.12).

5 Análise dos resultados

O capítulo de análise dos resultados permitirá, por cada objetivo, analisar quais as dificuldades encontradas na sua implementação, quais os resultados consequentes e quais as principais conclusões retiradas.

5.1 Plataforma

O estudo realizado para a Plataforma de gestão de configurações do laboratório 10 permitiu entender a complexidade da sua implementação. Essa complexidade começa com a variedade de equipamentos a incluir na plataforma.

Relativamente às funcionalidades disponíveis na plataforma, o processo mais complexo para o programa será a funcionalidade de envio de configurações para os equipamentos, pois existem diferentes tipos de equipamentos e isso vai exigir que o envio dos ficheiros seja adaptado para o funcionamento do próprio equipamento.

Na funcionalidade *download*, o programa vai armazenar as opções escolhidas pelo utilizador para o *download* de uma determinada configuração. As opções armazenadas serão inseridas na base de dados juntamente com o ficheiro, permitindo que possam ser facilitadas as outras funcionalidades da plataforma.

5.2 SmartRoom – Sensores

A análise de dados dos sensores será feita com recurso a imagens da plataforma de sensores, de modo a facilitar a explicação dos dados e demonstrar a estrutura dessa mesma plataforma. A análise será feita pela ordem apresentada no ponto 4.2.3.

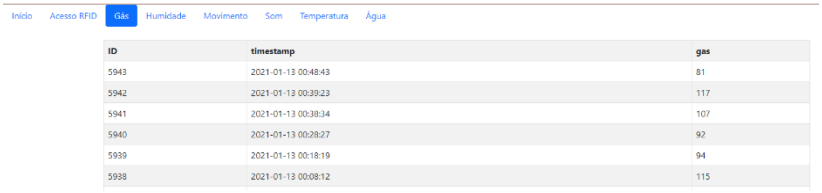


Figura 55 – Plataforma Sensores – Página Gás

A leitura deste sensor é importante na deteção de fumo em caso de incêndio na sala, entre outros. Se os valores detetados pelo sensor de gás ultrapassarem o valor 200, deverá despertar a atenção e a rápida verificação do possível incidente.

Figura 56 - Plataforma Sensores – Página Som

Os dados recolhidos pelo sensor de som permitem detetar situações menos normais do funcionamento da sala técnica. Essas situações podem passar pela deteção de excesso de pessoas dentro da sala técnica, não garantindo a segurança dos equipamentos, a queda de equipamentos dos locais onde estão fixos ou, até, no caso de existirem equipamentos com alarme, poderem ser detetados esses alarmes.

Os resultados demonstrados na Figura 56 foram recolhidos na sala técnica com alguns equipamentos ligados e sem o ar condicionado ligado, portanto, é importante salientar que os valores demonstrados podem aumentar conforme o número de equipamentos a funcionar.

Figura 57 - Plataforma Sensores – Página Temperatura

A recolha da temperatura é extremamente importante para detetar diversas anomalias que podem ocorrer na sala técnica. A temperatura pode sofrer variações significativas e vai depender da quantidade de equipamentos que estiverem em funcionamento em simultâneo e se os equipamentos de ar-condicionado estão ligados ou não. Como tal, os valores recolhidos podem indicar diversos cenários, tais como incêndio, a avaria dos equipamentos de ar-condicionado e, consequentemente, o sobreaquecimento dos equipamentos ligados ou até mesmo se a porta da sala técnica ficou aberta por algum motivo.

Os dados apresentados na figura 57 foram recolhidos na sala técnica, com os equipamentos de ar-condicionado desligados e apenas alguns equipamentos a funcionar.

Figura 58 - Plataforma Sensores – Página Humidade

O sensor que faz a leitura da humidade é o mesmo sensor que faz a leitura da temperatura. A presença de excessiva humidade poderá afetar os equipamentos, os seus componentes e acessórios. O nível de influência vai sempre depender da temperatura, isto é, quanto mais alta a temperatura e mais humidade exista no ar, mais graves serão as consequências para os equipamentos, desde corrosão a curto-circuitos.

Os dados apresentados de seguida foram recolhidos nas mesmas condições que os dados da temperatura, apresentados na Figura anterior.

As figuras 55 a 58 representam um módulo de sensores que foi implementado com um intervalo de leitura de 10 minutos. Este tempo foi definido apenas para testes, sendo o ideal na implementação final que os sensores estejam a ler os valores em contínuo mas enviam os valores para a base de dados se esses forem diferentes do último valor inserido, poupando trabalho ao Arduino, otimizando o espaço na base de dados e o tráfego gerado.

Figura 59 - Plataforma Sensores – Página Água

Os dados apresentados na Figura 59 são os valores recolhidos pelo sensor do nível de água. O objetivo deste módulo é saber se existe água no chão da sala, independentemente do nível da mesma. Com a medida digital só poderão ser lidos dois valores: zero ou um.

A simulação foi feita na sala técnica. A leitura deu valores constantes de zero, logo registamos que não houve qualquer incidente no período de testes. De salientar que também foi feita uma leitura com água numa chave de café para verificar o correto funcionamento do sensor.

A inserção do valor zero (não detetado) ou um (detetado) na base de dados foi feita apenas para motivos de teste. Numa situação real seria apenas inserido na base de dados um registo aquando da deteção de água, utilizando-se para esse efeito o campo do *timestamp* de forma a registar a data e hora da ocorrência.

Figura 60 - Plataforma Sensores – Página Movimento

O sensor de movimento tem como objetivo detetar movimento e ativar uma lâmpada. O módulo não foi montado, mas a simulação foi feita na sala técnica. Tal como explicado no ponto 4.2.3.3, o sensor enviará para a base de dados a leitura digital do sensor de movimento, isto é, o valor um. Logo, o valor inserido será sempre igual. Por fim, também foi testado

anteriormente, o sensor não deteta movimento para além do acrílico que divide a sala técnica da sala de aulas.

Para uma melhor gestão dos dados recolhidos e com base no funcionamento do sensor, concluiu-se que bastaria guardar na base de dados o campo do *timestamp* aquando da leitura do movimento.

Figura 61 - Plataforma Sensores – Página Acesso RFID

O módulo de controlo de acesso tem a função de registar quais os UIDs que foram autorizados a entrar, com base no que está descrito no código.

Apesar de o módulo não ter sido completamente implementado nas portas do laboratório 10, os testes foram feitos tanto com o cartão e o porta-chaves que vêm com o sensor, como também com cartões do ISMAI. Com esse teste foi possível concluir que o sensor também aceita cartões do ISMAI.

Os testes foram feitos com UIDs inseridos diretamente no código do Arduino. Numa situação real a verificação dos UIDs dos utilizadores do laboratório seria feita com uma consulta à base de dados presente no servidor, onde seria possível verificar se o utilizador em questão tem permissões ou não para aceder ao laboratório.

5.3 Relatório de Gestão do Risco

O Relatório de Gestão do Risco vai permitir perceber quais as medidas a adotar para melhorar a segurança do laboratório 10.

As respostas às perguntas presentes no Anexo 12 (ponto 9.12) são analisadas e compiladas no Relatório de Gestão de Risco do Laboratório de Redes e Sistemas Informáticos do ISMAI (laboratório 10) apresentado no Anexo 13 (ponto 9.13).

O Quadro Nacional de Referência para a Cibersegurança tem como função apresentar às organizações os requisitos mínimos a serem cumpridos por parte das mesmas, de forma a reduzir o risco associado à sua segurança digital. A análise do documento por parte da organização deverá com espírito crítico que tenha em consideração o contexto da mesma pois as organizações encontram-se, naturalmente, em diferentes níveis de maturidade. No relatório em causa, foi feita uma adaptação para o contexto do Laboratório 10, que não é uma organização, mas depende sempre da Maiêutica.

As medidas de segurança apresentadas no QNRCS são cinco: Identificar, Proteger, Detetar, Responder e Recuperar. O documento apresentado aborda as categorias e subcategorias do QNRCS no contexto do Laboratório 10 e as necessidades apresentadas pelos seus diferentes utilizadores.

O primeiro passo será aplicar a medida de segurança Identificar. Esta medida contempla a gestão dos ativos do laboratório 10, que passa pela identificação dos equipamentos, plataformas, redes e fluxos de dados. De seguida, é importante identificar-se o ambiente em que se encontra o laboratório 10, isto é, identificar os fornecedores, enumerar os ativos críticos, analisar os possíveis cenários de crise e, com isso, criar um ou vários planos de recuperação. A avaliação dos riscos é um ponto igualmente importante. Esta avaliação passa pela identificação e análise das vulnerabilidades e das ameaças internas e/ou externas. A gestão dos riscos passa pela criação de um processo onde são identificados os diversos responsáveis pelo processo em si e pelo tratamento desses riscos, com a criação de uma estratégia para o mesmo. Por fim, deve ser avaliada a tolerância ao risco do laboratório 10.

Na medida de segurança Proteger é importante que instituição tenha em conta a necessidade atual da melhoria do sistema de gestão de identidades, autenticação e controlos de acesso ao laboratório 10. Deverá ser criado um sistema de gestão de identidades e acessos que permita tipificar os utilizadores do laboratório 10, atribuindo critérios a cada um deles. A implementação de um controlo de acessos físico, de forma a ultrapassar o atual sistema,

através do uso de cartões eletrónicos ou um controlo equivalente. Também importante é o controlo de acessos remotos ao laboratório 10, sendo um método cada vez mais necessário por parte dos alunos e docentes, de forma a rentabilizar melhor o uso dos ativos e a suscitar nos alunos um mais forte interesse pelas cadeiras lecionadas. Nesta medida de segurança, é igualmente importante ter em conta a necessidade da instituição em formar e sensibilizar colaboradores de quais os seus papéis/responsabilidades perante e para com o laboratório 10. Relativamente à segurança dos dados, deve-se definir estratégias para garantir a confidencialidade e integridade da informação que circula no laboratório 10. Estes critérios só poderão ser cumpridos se os ativos forem capazes e, por isso, é importante a instituição garantir que os contratos com os fornecedores dos ativos garantam a manutenção e reparação dos mesmos.

A medida de segurança Detetar abrange a necessidade de a instituição criar métodos de monitorização das redes e sistemas de informação do laboratório 10 de forma a detetar eventos, coletá-los e correlacioná-los. Este processamento permitirá perceber qual o impacto dos mesmos e a possibilidade de os mesmos se tornarem incidentes. No processo de deteção também deverão ser definidos os responsáveis por essa mesma deteção. A monitorização também deverá ser aplicada no ambiente físico, com o uso de CCTV e controlos de acesso. Também se deverá criar sistemas de deteção de código malicioso, importante para a disponibilidade e integridade dos ativos do laboratório 10.

A medida de segurança Responder contempla a necessidade de a instituição criar um plano de resposta a todos os eventos detetados na medida de segurança anterior. Esse plano deverá ser constituído, também, por um processo de resolução de incidentes, onde deverão estar explícitos os responsáveis pelo tratamento de incidentes, que farão a distribuição dos recursos durante o processo de resolução. A análise de evidências também está incluída neste plano, sendo necessário manter a sua integridade, de forma a que se possa fazer análises de diferentes níveis. Após a execução da resposta a esse incidente, é necessário avaliar o impacto desse mesmo incidente no laboratório 10 e fazer a categorização do mesmo com base na Taxonomia Nacional, referenciada neste documento. Após os incidentes serem contidos,

deve-se identificar as novas vulnerabilidades e a instituição terá de executar ações de correção dessas vulnerabilidades ou justificar a aceitação dos riscos.

Por fim, mas não menos importante, a medida de segurança de Recuperar. Esta medida contempla a execução de um plano de recuperação de incidentes, que deve ser implementado durante ou após o ou os incidentes. Este plano deverá ser revisto com regularidade. Após a execução do plano de recuperação, deverá ser criado um plano de melhorias, durante o qual se executa as ações resultantes das lições aprendidas. Ao longo de todo o documento foi várias vezes mencionada a importância da existência de um plano de comunicação de vulnerabilidades e incidentes.

As principais conclusões retiradas e explicadas na análise anterior são:

- Necessidade de documentar oficialmente quais os dispositivos físicos, redes e sistemas de informação presentes no laboratório 10;
- Identificar as aplicações e plataformas de *software* que suportam os serviços críticos das redes e fluxos de dados do laboratório 10;
- Identificar os ativos críticos e adoção de medidas para a proteção dos mesmos dependendo da necessidade identificada (UPS e sistemas AVAC);
- Identificar cenários de crise e planos de recuperação;
- Identificar vulnerabilidades dos ativos e das ameaças internas e externas;
- Implementação de medidas de controlo de acesso a todas as redes e sistemas de informação do laboratório 10;
- Formação dedicada aos colaboradores docentes e não docentes do ISMAI;
- Monitorização do perímetro físico do laboratório 10 (CCTV, controlo de acesso);
- Monitorização do laboratório e da sala técnica que permita perceber quais as condições em que os equipamentos do laboratório estão inseridos, podendo serem detetadas anomalias.

6 Conclusões

A criação do novo laboratório de redes e sistemas informáticos do ISMAI, com uma sala técnica própria, fez com que surgissem algumas necessidades a nível de gestão e segurança da mesma. Com o melhoramento das condições de ensino (com a aquisição de novos equipamentos e aumento do espaço), também houve um aumento das dificuldades na gestão dos equipamentos da sala.

A idealização da plataforma de gestão das configurações do laboratório 10 permitiu entender o processo necessário para a criação da mesma, ou seja, a informação que a pessoa que a construir necessitará para a sua implementação e quais os pontos fundamentais dessa mesma implementação. A explicação do funcionamento permitiu aplicar conhecimentos adquiridos anteriormente mas também a pesquisa do funcionamento de equipamentos com os quais raramente houve contacto durante o curso, por isso, é importante salientar que a implementação desta plataforma deve ser adaptada aos testes que forem decorrendo ao longo dessa mesma implementação.

As redes de sensores são extremamente importantes no que toca a uma boa gestão de um determinado ambiente. Tornar uma sala numa *smartroom* traz muitas vantagens desde a automação da monitorização das condições da sala, a controlos de acesso, entre outros. Ao longo do projeto, que sofreu percalços derivados da situação atípica do ano anterior e do atual, foi possível implementar três módulos de sensores (4.2.3.1, 4.2.3.2 e 4.2.3.3). Os dados recolhidos desses sensores estão todos em situações normais, provando que não se registou informação que apontasse para acontecimentos que prejudicassem o ambiente em que os equipamentos se encontram, no período de teste dos sensores.

Por fim, a gestão do risco é extremamente importante para uma organização que tem uma determinada atividade das quais várias pessoas possam depender. Foi criado um relatório de gestão do risco com base no Quadro Nacional de Referência para a Cibersegurança adaptado ao laboratório 10. Para a construção deste relatório fez-se um questionário aos colaboradores que trabalham no laboratório 10. Este questionário permitiu saber sobre o laboratório e de que forma os colaboradores avaliam a segurança do mesmo e

dos equipamentos. Os resultados obtidos pelos inquiridos permitem concluir que existem lacunas na estrutura do mesmo, em termos físicos e lógicos. Após a identificação dos possíveis cenários de crise, é possível entender que a disponibilidade da sala técnica do laboratório 10 é extremamente importante. Esta disponibilidade estará sempre em causa, mas há algumas medidas que poderão ser implementadas de forma a garanti-la, incluindo proteção do fornecimento de energia aos equipamentos no caso de falha de eletricidade. É também de salientar a importância da segurança da infraestrutura com o uso de CCTV e controlos de acesso, assim como a formação dos colaboradores envolvidos sobre boas práticas para o bom funcionamento do espaço.

Em suma, foi possível entender que o laboratório 10 é um espaço cada vez mais importante para a instituição e para todos os docentes e alunos da área em questão.

7 Trabalho Futuro

O projeto sofreu alterações e adaptações devido à situação atípica vivida nos anos de 2020 e 2021. Com isto, é possível perceber que este trabalho tem potencial para a execução de projetos futuros.

Como referido anteriormente, a plataforma de gestão de configurações é extremamente importante para melhorar as condições de utilização do laboratório 10, pelo que a sua implementação seria uma mais valia.

A implementação de um conjunto de sensores num determinado ambiente é extremamente versátil por as redes de sensores modernas serem modulares e baseadas em protocolos abertos, permitindo um elevado grau de escalabilidade e evolução. No caso deste projeto, uma das otimizações a implementar poderá ser ao nível do código do Arduino permitindo que os valores detetados pelos sensores do módulo do ponto 4.2.3.1 sejam inseridos na base de dados apenas quando os mesmos forem diferentes do último valor inserido, ao contrário do atualmente implementado, que é a recolha de dados de 10 em 10 minutos. Nos sensores de água e movimento a alteração que poderá ser implementada é a remoção de colunas nas tabelas da base de dados. Por fim, a implementação física do módulo de controlo de acessos permitindo, desta forma, um melhor controlo das autorizações atribuídas aos utilizadores do laboratório 10 e o acréscimo de outros sensores, nomeadamente, um sensor de corrente que permita monitorizar a corrente consumida pela zona técnica.

Por fim, o relatório de gestão do risco fez entender quais os riscos que o laboratório 10 pode sofrer, principalmente, os equipamentos disponíveis na sala técnica. Portanto, é importante iniciar um processo de implementação de medidas para a proteção dos mesmos, sendo que a implementação destas medidas exige que seja devidamente documentada toda a informação necessária para se entender qual os possíveis cenários de risco, vulnerabilidades e ameaças. As medidas devem ser implementadas de forma calma e concisa, não dando espaço para lacunas que prejudiquem a própria implementação da gestão do risco.

8 Referências

1 Channel 5V Relay Shield Module. (n.d.). Retrieved January 15, 2021, from https://www.ptrobotics.com/modulos-de-reles/3635-1-channel-5v-relay-shield-module.html?gclid=CjwKCAiAl4WABhAJEiwATUnEF68M8JqyrL17neV19BDAxC54ru8Uw8g7U3lmv3031JJrc6I7SpKfYBoCebIQAvD_BwE

Ada, Lady. (2020). Adafruit Learning System: PIR Motion Sensor. In *Adafruit Learning System* (pp. 1–28). https://cdn-learn.adafruit.com/downloads/pdf/pir-passive-infrared-proximity-motion-sensor.pdf?timestamp=1585441256

Al-falahy, N., & Alani, O. Y. (2017). *Technologies for 5G Networks : Challenges and Opportunities*.

Al-kahtani, M. A., & Sandhu, R. (2002). *A Model for Attribute-Based User-Role Assignment*.

Aosong Electronics. (2010). Temperature and Humidity Module, AM1001. *Datasheet*, 9.

Arduino - Setting up an Arduino on a breadboard. (n.d.). Retrieved January 15, 2021, from https://www.arduino.cc/en/main/standalone

Arduino Nano | Arduino Official Store. (n.d.). Retrieved January 15, 2021, from https://store.arduino.cc/arduino-nano

Ashraf, Q. M., Habaebi, M. H., Islam, M. R., & Khan, S. (2016). Device discovery and configuration scheme for Internet of Things. *2016 International Conference on Intelligent Systems Engineering, ICISE 2016*, 38–43. https://doi.org/10.1109/INTELSE.2016.7475159

Assembleia da República. (2018a). *Lei 46/2018, 2018-08-13 - DRE*. https://dre.pt/home/-/dre/116029384/details/maximized

Assembleia da República. (2018b). *Política Geral de Segurança da Informação da Assembleia da República*. 1–5.

Barbosa Cabral, J. L. (2017). *Massive MIMO*. ISCTE-IUL.

Bastos, A. V., & Cecílio, D. (2017). *Minicurso - Comunicação D2D para 5G de Arquiteturas de Redes Celulares : Da Teoria à Prática* (Issues 1–30). https://doi.org/10.13140/RG.2.2.18432.12807

Beatrys Ruiz, L., A. Correia, L. H., M. Vieira, L. F., F. Macedo, D., F. Nakamura, E., M. S. Figueiredo, C., M. Vieira, M. A., Habib Bechelane, E., Camara, D., A. F. Loureiro, A., S. Nogueira, J. M., C. da Silva Jr., D., & O. Fernandes, A. (2004). Arquiteturas para Redes de Sensores sem Fio. In *Arquiteturas para Redes de Sensores sem Fio*.

Breadboard Power Supply Module 3.3V/5V. (n.d.). Retrieved January 15, 2021, from https://www.ptrobotics.com/alimentacao/5924-breadboard-power-supply-module-33v-5v.html?gclid=CjwKCAiAl4WABhAJEiwATUnEF5G9RMJfNchWOLKHdrOkpKX5GpvympvLEjphNtAjuFstalzapx466hoCOEkQAvD_BwE

Centro Nacional de Cibersegurança. (2019). *Quadro Nacional de Referência para a Cibersegurança*. https://www.cncs.gov.pt/content/files/cncs_qnrcs_2019.pdf

Chess, D. M., & Kephart, J. O. (2003). The Vision of Autonomic Computing. *Computer*, *36*(January), 41–50. https://doi.org/10.1046/j.1365-2745.2002.00730.x

Chung, A., Dawda, S., Hussain, A., Shaikh, S. A., & Carr, M. (2014). Cybersecurity: Policy. In *Encyclopedia of Security and Emergency Management* (Vol. 1, pp. 1–15). https://doi.org/10.1007/978-3-319-69891-5_20-1

Comissão Europeia. (2016a). DIRETIVA (UE) 2016/1148 DO PARLAMENTO EUROPEU E DO CONSELHO de 6 de julho de 2016. *Official Journal of the European Union*, *2014*(2), 1–30. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148

Comissão Europeia. (2016b). *L_2016119PT.01000101.xml*. Jornal Oficial Da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679

Conference, I., & Systems, I. (2018). *Automatic Integration of IoT Devices* (Issue 351).

DHT11 Sensor Pinout, Features, Equivalents & Datasheet. (n.d.). Retrieved January 15, 2021, from https://components101.com/dht11-temperature-sensor

diagrams.net. (n.d.). Retrieved January 20, 2021, from https://app.diagrams.net/

Display LCD 16x2 I2C com fundo azul. (n.d.). Retrieved January 15, 2021, from https://www.electrofun.pt/display/display-lcd-16x2

DSSS - Direct Sequence Spread Spectrum - YouTube. (n.d.). Retrieved January 20, 2020,

from https://www.youtube.com/watch?v=-1mxYWvfVWQ&list=WL&index=13&t=0s

ENISA. (2018). Reference Incident Classification Taxonomy Task Force Status and Way Forward. In *European Union Agency For Network and Information Security* (Issue January, p. 20).

FE & MO TECHNOLOGY S.L.U. (n.d.). Retrieved January 15, 2021, from https://www.moveteck.com/producto/0751572/GT882-NE-Cargador-Universal-BM-24W-con-1USB-6W%2C-3V-12V-2A-con-6-tips

FHSS - Frequency Hopping Spread Spectrum - YouTube. (n.d.). Retrieved January 20, 2020, from https://www.youtube.com/watch?v=CkhA7s5GIGc&list=WL&index=12&t=271s

Gil, J. M. V. S. (2012). *Monitorização, Alarmística e Gestão de Redes*. Instituto Politécnico de Leiria.

Glória, A., Cercas, F., & Souto, N. (2017). Design and implementation of an IoT gateway to create smart environments. In *Procedia Computer Science*. https://doi.org/10.1016/j.procs.2017.05.343

Guedes, G. T. A. (2018). *UML 2 - Uma Abordagem Prática - Gilleanes T. A. Guedes - Google Livros* (Novatec (Ed.); 3ª). https://books.google.com.br/books?hl=pt-PT&lr=&id=mJxMDwAAQBAJ&oi=fnd&pg=PA2&dq=diagramas+da+uml&ots=x9sQPiXOl0&sig=_sJSXHEV6xFn2FqI8WfyhC5uuvs#v=onepage&q=diagramas da uml&f=false

H. Mahmoud, Q. (2007). *Congnitive Networks - Towards Self-Aware Netowrks*.

Haartsen, J. (1998). Bluetooth - the universal radio interface for ad hoc, wireless connectivity. *Ericsson Review (English Edition)*, *75*(3), 110–117.

Handsontec. (2017). Handson Technology. *Hanson Technology*, 1–22. http://www.handsontec.com/pdf_learn/esp8266-V10.pdf

IEC. (2016). *ISO/IEC 20922:2016 | IEC Webstore*. https://webstore.iec.ch/publication/25096

IEEE. (2019). *P802.15.4-REVd/D04, Oct 2019 - IEEE Draft Standard for Low-Rate Wireless*

Networks (WPANs) - IEEE Standard. https://ieeexplore.ieee.org/document/8935588?denied=

IREO - Distribuidor de Soluções TI. (2019). *ManageEngine*. https://www.ireo.com/pt/fabricantes-e-produtos/manageengine

ISO/IEC. (2012). *ISO/IEC 27032:2012(en), Information technology — Security techniques — Guidelines for cybersecurity*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

ISO/IEC. (2018a). *ISO/IEC 27005:2018(en), Information technology — Security techniques — Information security risk management*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en

ISO/IEC. (2018b). *Risk management ISO 31000*.

Jaouhari, S. E. L., Palacios-Garcia, E. J., Anvari-Moghaddam, A., & Bouabdallah, A. (2019). Integrated management of energy, wellbeing and health in the next generation of smart homes. In *Sensors (Switzerland)* (Vol. 19, Issue 3). https://doi.org/10.3390/s19030481

Keeler, J. (2004). MFRC522: Contactless Reader IC. *Understanding NMR Spectroscopy*, *May*, 1-1-1–3.

Khan, P. M., & Quraishi, K. A. (2014). Impact of RACI on delivery and outcome of software development projects. *International Conference on Advanced Computing and Communication Technologies, ACCT*, 177–184. https://doi.org/10.1109/ACCT.2014.66

Kim, E., Kaspar, D., Gomez, C., & Bormann, C. (2012). Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing. In *RFC6606*.

Lampson, B. W. (1974). Protection. *Information Sciences*, 18–24.

Liikanen, J., Stoneman, P., & Toivanen, O. (2004). Intergenerational effects in the diffusion of new technology: The case of mobile phones. *International Journal of Industrial Organization*, *22*(8–9), 1137–1154. https://doi.org/10.1016/j.ijindorg.2004.05.006

ManageEngine NCM. (n.d.). *Schedule network device configuration backup*. Retrieved November 17, 2019, from https://www.manageengine.com/network-configuration-

manager/scheduling-configuration-tasks.html

Marques, A. F. C. (2015). *Desenho e Implementação de uma Plataforma Integrada para Monitorização e Gestão de uma Rede de um Departamento da UMa* [Universidade da Madeira]. https://digituma.uma.pt/bitstream/10400.13/1246/1/MestradoAndreiaMarques.pdf

Microchip Technology Inc. (2006). Data Sheet Stand-Alone Ethernet Controller with SPI Interface. *Technology*.

Módulo Leitor RFID RC522 Arduino. (n.d.). Retrieved January 15, 2021, from https://www.electrofun.pt/comunicacao/leitor-rfid-arduino

Mukherjee, S., & Biswas, G. P. (2018). Networking for IoT and applications using existing communication technology. *Egyptian Informatics Journal*, *19*(2), 107–127. https://doi.org/10.1016/j.eij.2017.11.002

Myers, A. C., & Liskov, B. (1997). *A decentralized model for information flow control*. https://doi.org/10.1145/268998.266669

NIST. (2018). Framework for improving critical infrastructure cybersecurity. *Proceedings of the Annual ISA Analysis Division Symposium*, *535*, 9–25.

Office of the Law Revision Counsel of the U.S. House of Representatives. (1968). *44 U.S. Code CHAPTER 35— COORDINATION OF FEDERAL INFORMATION POLICY Subchapter II § 3552. Definitions*. 3553. https://www.law.cornell.edu/uscode/text/44/3552

Olimex. (2013). Tecnical Data Mq-135 Gas Sensor. In *Hanwei Electron* (Vol. 1, pp. 3–4).

P. Pfleeger, C., Lawrence Pfleeger, S., & Margulies, J. (2015). *Security in Computing*.

Patino, S., Solis, E. F., Yoo, S. G., & Arroyo, R. (2018). ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO/IEC 27005. *2018 5th International Conference on EDemocracy and EGovernment, ICEDEG 2018*, 75–82. https://doi.org/10.1109/ICEDEG.2018.8372361

Patrick Kinney. (2003). ZigBee Technology : Wireless Control that Simply Works. *Communications Design Conference, October*, 1–20.

Paulsen, C. Toth, P. (2016). Small Business Information Security: The Fundamentals Small

Business. In *National Institute of Standards and Technology Interagency Report* (Vol. 7621, p. 54). https://doi.org/10.6028/NIST.IR.7621r1

Philips. (2002). *Data Sheet PCF8574* (pp. 0–24). http://www.papersearch.net/view/detail.asp?detail_key=10000715

Pires, J. (2018). *Gestão técnica e operacional da rede metropolitana da Associação Porto Digital*.

Ruiz, L. B. (2003). *Maná: uma arquitetura para gerenciamento de redes de sensores sem fio*. http://www2.dcc.ufmg.br/~linnyer/TeseMANNA.pdf%5Cnhttp://www2.dcc.ufmg.br/%7B~%7Dlinnyer/TeseMANNA.pdf

Sá Silva, J., Mendão Silva, R., & Boavida, F. (2016). *Redes de Sensores sem Fios - Informática - Redes & Comunicações - FCA*. 2016. https://www.fca.pt/pt/catalogo/informatica/redes-comunicacoes/redes-de-sensores-sem-fios/

Saha, S., & Majumdar, A. (2017). Data centre temperature monitoring with ESP8266 based Wireless Sensor Network and cloud based dashboard with real time alert system. *Proceedings of 2nd International Conference on 2017 Devices for Integrated Circuit, DevIC 2017*, 307–310. https://doi.org/10.1109/DEVIC.2017.8073958

Saleiro, M., & Ey, E. (2009). *ZigBee uma abordagem prática*.

Sensor de Gases MQ-135. (n.d.). Retrieved January 17, 2021, from https://www.botnroll.com/pt/biometricos/2195-sensor-de-gases-mq-135.html

Sensor de Som c/ saída Analógica e Digital. (n.d.). Retrieved January 15, 2021, from https://www.botnroll.com/pt/som/2162-sensor-de-som-c-saida-analogica-e-digital.html

Sensor PIR / Sensor Movimento para Arduino. (n.d.). Retrieved January 15, 2021, from https://www.electrofun.pt/sensores-arduino/sensor-movimento-pir-arduino

Shelby, Z., & Bormann, C. (2011). The Wireless Embedded Internet. In *Annals of CASE* (Vol. 43). http://www.sase.com.ar/2011/files/2011/02/59-Wireless_Embedded_Internet_6LowPan.pdf

SHENZHEN RUITE ELECTRONIC CO., L. (n.d.). *RT162-7* (p. 1).

SolarWinds. (2019). *Software de gerenciamento de TI e ferramentas de monitoramento*.

Souza, L. De, Rosa, P., Barcelos, R. G., Pereira, Y., & Real, Y. (2017). *Aplicações do 5G em Internet das Coisas (IoT)*.

Systems, C. on N. S. (2015). *Committee on National Security Systems (CNSS) Glossary* (Issue 4009, pp. 1–165). https://doi.org/10.1201/9780203888933.ch13

Tahir, M., Mamoon Ashraf, Q., & Dabbagh, M. (2019). Towards enabling autonomic computing in IoT ecosystem. *Proceedings - IEEE 17th International Conference on Dependable, Autonomic and Secure Computing, IEEE 17th International Conference on Pervasive Intelligence and Computing, IEEE 5th International Conference on Cloud and Big Data Computing, 4th Cyber Scienc, August*, 646–651. https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00122

Teixeira De Gouveia, B. A. (2009). *Dispositivos de Monitorização e Controlo automático de fatores climáticos em Museus*. Universidade da Madeira.

Thomas, P., & Kumar, J. P. (2019). Cloud Based Dynamic Energy Management in Power System Using Message Queuing Telemetry Transport (MQTT) Protocol. *Proceedings of the 3rd International Conference on Electronics and Communication and Aerospace Technology, ICECA 2019*, 1301–1305. https://doi.org/10.1109/ICECA.2019.8821818

Ubidots. (2020). *IoT platform | Internet of Things*. https://ubidots.com/

VMA303: MÓDULO DE SENSOR DE HUMIDADE DO SOLO & SENSOR DE NÍVEL DE ÁGUA – Velleman – Wholesaler and developer of electronics. (n.d.). Retrieved January 15, 2021, from https://www.velleman.eu/products/view?id=435520&country=be&lang=pt

Wheeler, A. (2007). Commercial applications of wireless sensor networks using ZigBee. *IEEE Communications Magazine*, *45*(4), 70–77. https://doi.org/10.1109/MCOM.2007.343615

Xu, K., Wan, Y., & Xue, G. (2019). Powering Smart Homes with Information-Centric Networking. *IEEE Communications Magazine*, *57*(6), 40–46. https://doi.org/10.1109/MCOM.2019.1800732

Yassein, M. B., Mardini, W., & Khalil, A. (2016). Smart homes automation using Z-wave protocol. *Proceedings - 2016 International Conference on Engineering and MIS, ICEMIS 2016*, 1–6. https://doi.org/10.1109/ICEMIS.2016.7745306

Yuan, M. (2017). *Conhecendo o MQTT*. https://www.ibm.com/developerworks/br/library/iot-mqtt-why-good-for-iot/index.html

Z-wave. (2019). *Introduction to Z-Wave - An Introductory Guide to Z-Wave Technology*.

Z-Wave. (2019). *Introduction to Z-Wave - An Introdutory Guide to Z-Wave Technology*.

Zheng, J., Simplot-ryl, D., Bisdikian, C., & Mouftah, H. T. (2011). The internet of things [Guest Editorial]. In *IEEE Communications Magazine* (Vol. 49, Issue November). IEEE. https://doi.org/10.1109/MCOM.2011.6069706

9 Anexos

9.1 Anexo 1 – Código Arduino do Módulo de Sensores de Som, Gás e DHT11

```
#include "DHT.h"
#include <UIPEthernet.h>
#define DHTPIN 4
#define DHTTYPE DHT11
uint8_t mac[6] = { 0x74,0x69,0x69,0x3D,0x33,0x33 };
IPAddress myIP(192,168,201,21);
IPAddress server(192,168,201,22);
IPAddress subnet(255,255,255,0);
EthernetClient client;
DHT dht(DHTPIN, DHTTYPE);
int smokeA1 = A1;
int soundA5 = A5;
void setup() {
  Serial.begin(115200);
  Serial.println("Chegou aqui!!");
  Ethernet.begin(mac, myIP, server, subnet);
  dht.begin();
  delay(1000);
  pinMode(smokeA1,INPUT);
  pinMode(soundA5,INPUT);
}
void loop() {
gasR();
delay(2000);
soundR();
```

```
delay(2000);
temR();
delay(2000);
humR();
unsigned long startTimestamp;
unsigned long timestamp;
const unsigned long timer_length = 600000; //10 seconds
startTimestamp = millis();
timestamp = startTimestamp;
while ( (timestamp - startTimestamp) < timer_length){
   timestamp = millis();
}
}
void gasR() {
int gasSensor = analogRead(smokeA1);
if (client.connect(server, 80)) {
Serial.println("connected");
client.print("GET /sensors/gasSensor.php?");
client.print("gas=");
client.print(gasSensor);
client.print(" HTTP/1.1\r\n");
client.println("Host: 192.168.201.22\r\n");
Serial.print("gas= ");
Serial.println(gasSensor);
client.stop();
}
else {
Serial.println("falha na conexão");
}
```

```
}
void soundR() {
int soundSensor = analogRead(soundA5);
if (client.connect(server, 80)) {
Serial.println("connected");
client.print("GET /sensors/soundSensor.php?");
client.print("sound=");
client.print(soundSensor);
client.print(" HTTP/1.1\r\n");
client.println("Host: 192.168.201.22\r\n");
Serial.print("som= ");
Serial.println(soundSensor);
client.stop();
}
else {
Serial.println("falha na conexão");
}
}
void humR(){
float h = dht.readHumidity();
if (client.connect(server, 80)) {
Serial.println("connected");
client.print("GET /sensors/humSensor.php?");
client.print("hum=");
client.print(h);
client.print(" HTTP/1.1\r\n");
client.println("Host: 192.168.201.22\r\n");
Serial.print("humidade= ");
Serial.println(h);
```

```
client.stop();
} else {
Serial.println("falha na conexão");
}
}
void temR(){
float t = dht.readTemperature();
if (client.connect(server, 80)) {
Serial.println("connected");
client.print("GET /sensors/temSensor.php?");
client.print("tem=");
client.print(t);
client.print(" HTTP/1.1\r\n");
client.println("Host: 192.168.201.22\r\n");
Serial.print("temperatura= ");
Serial.println(t);
client.stop();
}
else {
Serial.println("falha na conexão");
}
}
```

9.2 Anexo 2 – Código Arduino do Módulo de Sensor do Nível de Água

```
#include <UIPEthernet.h>
uint8_t mac[6] = { 0x74,0x69,0x69,0x3D,0x33,0x33 };
IPAddress myIP(192,168,201,23);
IPAddress server(192,168,201,22);
IPAddress subnet(255,255,255,0);
EthernetClient client;
int waterSensor = 4;
void setup () {
  Serial.begin(115200);
  Serial.println("Chegou aqui!!");
  Ethernet.begin(mac, myIP, server, subnet);
  delay(1000);
  pinMode (waterSensor,INPUT);
}
void loop() {
int water = digitalRead (waterSensor);
if (client.connect(server, 80)) {
Serial.println("connected");
client.print("GET /sensors/waterSensor.php?");
client.print("valor=");
client.print(water);
client.print(" HTTP/1.1\r\n");
client.println("Host: 192.168.201.22\r\n");
Serial.print("valor= ");
Serial.println(water);
```

```
client.stop();
} else {
Serial.println("falha na conexão");
}
delay(2000);
}
```

9.3 Anexo 3 – Código Arduino do Módulo de Sensor de Movimento

```
#include <UIPEthernet.h>
uint8_t mac[6] = { 0x74,0x69,0x69,0x3D,0x33,0x33 };
IPAddress myIP(192,168,201,25);
IPAddress server(192,168,201,22);
IPAddress subnet(255,255,255,0);
EthernetClient client;
int lamp = 5;
int inputPin = 6;
void setup() {
Serial.begin(115200);
Serial.println("Chegou aqui!!");
Ethernet.begin(mac, myIP, server, subnet);
delay(1000);
pinMode(lamp, OUTPUT);
pinMode(inputPin, INPUT);
}
void loop(){
int val = digitalRead(inputPin);
Serial.println(val);
```

```
if( val== 1) {
  digitalWrite(lamp,HIGH);
  if (client.connect(server, 80)) {
     Serial.println("connected");
     client.print("GET /sensors/pirSensor.php?");
     client.print("pir=");
     client.print(val);
     client.print(" HTTP/1.1\r\n");
     client.println("Host: 192.168.201.22\r\n");
     Serial.print("pir= ");
     Serial.println(val);
     client.stop();
    }
    else {
     Serial.println("falha na conexão");
    }
    } else {
     digitalWrite(lamp,LOW);
    }
delay(2000);
}
```

9.4 Anexo 4 – Código Arduino do Módulo de Sensor RFID

```
#include <MFRC522.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <SPI.h>
#include <UIPEthernet.h>
```

```
#define SS_PIN 5
#define RST_PIN 9
MFRC522 mfrc522(SS_PIN, RST_PIN);
LiquidCrystal_I2C lcd = LiquidCrystal_I2C(0x3F, 16, 2);
uint8_t mac[6] = { 0x74, 0x69, 0x69, 0x3D, 0x33, 0x33 };
IPAddress myIP(192, 168, 201, 27);
IPAddress server(192, 168, 201, 22);
IPAddress subnet(255, 255, 255, 0);
EthernetClient client;
unsigned char buffer[100];
char st[20];
void setup() {
  Serial.begin(115200);
  SPI.begin();
  mfrc522.PCD_Init();
    Ethernet.begin(mac, myIP);
  delay(6000);
  Serial.println(Ethernet.localIP());
  delay(2000);
  Serial.println("Aproxime o seu cartao do leitor...");
  Serial.println();
  lcd.begin(16, 2);
  mensageminicial();
}
void loop() {
  if ( ! mfrc522.PICC_IsNewCardPresent())
  {    return;  }
  if ( ! mfrc522.PICC_ReadCardSerial())
```

```
  {     return;  }
  String conteudo= "";
  byte letra;
  for (byte i = 0; i < mfrc522.uid.size; i++) {
     Serial.print(mfrc522.uid.uidByte[i], HEX);
     conteudo.concat(String(mfrc522.uid.uidByte[i], HEX));
  }
  Serial.println();
  conteudo.toUpperCase();
if (conteudo == "2CF35143" || conteudo == "45ECD283") {
    Serial.println("Bem Vindo/a!");
    Serial.println();
    lcd.clear();
    lcd.setCursor(0,0);
    lcd.print("Bem Vindo/a!");
  if (client.connect(server, 80)) {
      Serial.println("connected");
      client.print("GET /sensors/rfidSensor.php?");
      client.print("card=");
      client.print(conteudo);
      client.print(" HTTP/1.1\r\n");
      client.println("Host: 192.168.201.22\r\n");
Serial.print("card= ");
Serial.println(conteudo);
        client.stop();
        } else {
Serial.println("falha na conexão");
}
    delay(2000);
```

```
mensageminicial();
  Serial.println("Aproxime o seu cartao do leitor...");
  Serial.println();
} else {
    Serial.println("Acesso negado");
    Serial.println();
    lcd.clear();
    lcd.setCursor(0,0);
    lcd.print("Acesso negado!");
    delay(3000);
    mensageminicial();
    delay(2000);
  Serial.println("Aproxime o seu cartao do leitor...");
  Serial.println();
  }
}
void mensageminicial() {
  lcd.init();
  lcd.backlight();
  lcd.print(" Aproxime o seu");
  lcd.setCursor(0,1);
  lcd.print("cartao do leitor");
}
```

9.5 Anexo 5 – Código PHP do Sensor de Gás

```
<?php
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'root');
```

```
define('DB_PASSWORD', '');
define('DB_NAME', 'sensors');
$link = mysqli_connect(DB_SERVER, DB_USERNAME, DB_PASSWORD,
DB_NAME);
 if($link === false){
   die("ERROR: Could not connect. " . mysqli_connect_error());
}
$sql = "INSERT INTO gas (timestamp, gas) VALUES (CURRENT_TIMESTAMP,
'".$_GET["gas"]."')";
mysqli_query($link, $sql);
?>
```

9.6 Anexo 6 – Código PHP do Sensor de Som

```
<?php
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'root');
define('DB_PASSWORD', '');
define('DB_NAME', 'sensors');
$link = mysqli_connect(DB_SERVER, DB_USERNAME, DB_PASSWORD,
DB_NAME);
if($link === false){
   die("ERROR: Could not connect. " . mysqli_connect_error());
}
$sql = "INSERT INTO sound (timestamp, sound) VALUES (CURRENT_TIMESTAMP,
'".$_GET["sound"]."')";
   mysqli_query($link, $sql);
?>
```

9.7 Anexo 7 – Código PHP do Sensor DHT11 – Humidade

```
<?php
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'root');
define('DB_PASSWORD', '');
define('DB_NAME', 'sensors');
$link = mysqli_connect(DB_SERVER, DB_USERNAME, DB_PASSWORD, DB_NAME);
if($link === false){
   die("ERROR: Could not connect. " . mysqli_connect_error());
}
$sql = "INSERT INTO hum (timestamp, hum) VALUES (CURRENT_TIMESTAMP, '".$_GET["hum"]."')";
mysqli_query($link, $sql);
?>
```

9.8 Anexo 8 – Código PHP do Sensor DHT11 – Temperatura

```
<?php
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'root');
define('DB_PASSWORD', '');
define('DB_NAME', 'sensors');
$link = mysqli_connect(DB_SERVER, DB_USERNAME, DB_PASSWORD, DB_NAME);
 if($link === false){
   die("ERROR: Could not connect. " . mysqli_connect_error());
}
```

```
$sql = "INSERT INTO tem (timestamp, tem) VALUES (CURRENT_TIMESTAMP, '".$_GET["tem"]."')";
    mysqli_query($link, $sql);
?>
```

9.9 Anexo 9 – Código PHP do Sensor do Nível de Água

```
<?php
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'root');
define('DB_PASSWORD', '');
define('DB_NAME', 'sensors');
$link = mysqli_connect(DB_SERVER, DB_USERNAME, DB_PASSWORD, DB_NAME);
if($link === false){
   die("ERROR: Could not connect. " . mysqli_connect_error());
}

$sql = "INSERT INTO water (timestamp, value) VALUES (CURRENT_TIMESTAMP, '".$_GET["value"]."')";
 mysqli_query($link, $sql);
?>
```

9.10 Anexo 10 – Código PHP do Sensor de Movimento

```
<?php
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'root');
define('DB_PASSWORD', '');
```

```
define('DB_NAME', 'sensors');
$link = mysqli_connect(DB_SERVER, DB_USERNAME, DB_PASSWORD, DB_NAME);
if($link === false){
   die("ERROR: Could not connect. " . mysqli_connect_error());
}
$sql = "INSERT INTO pir (timestamp, pir) VALUES (CURRENT_TIMESTAMP, '".$_GET["pir"]."')";
 mysqli_query($link, $sql);
?>
```

9.11 Anexo 11 – Código PHP do Sensor de RFID

```
<?php
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'root');
define('DB_PASSWORD', '');
define('DB_NAME', 'sensors');
 $link = mysqli_connect(DB_SERVER, DB_USERNAME, DB_PASSWORD, DB_NAME);
 if($link === false){
   die("ERROR: Could not connect. " . mysqli_connect_error());
}
$sql = "INSERT INTO accessrfid1 (timestamp, card) VALUES (CURRENT_TIMESTAMP, '".$_GET["card"]."')";
   mysqli_query($link, $sql);
?>
```

9.12 Anexo 12 – Perguntas Questionário sobres Gestão do Risco no Laboratório 10

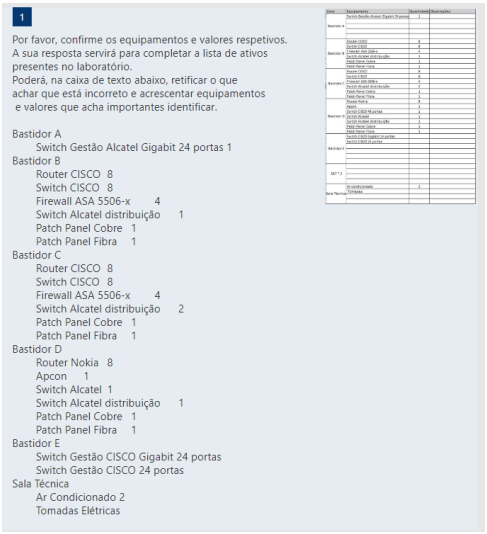


Figura 62 – Questionário Gestão do Risco – Pergunta 1

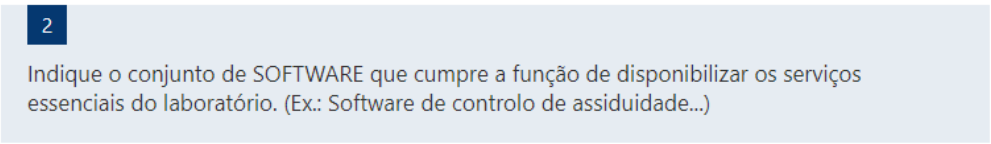


Figura 63 - Questionário Gestão do Risco – Pergunta 2

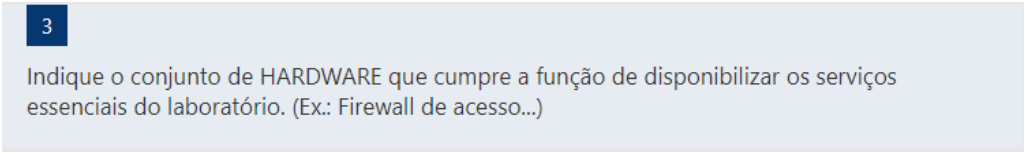


Figura 64 - Questionário Gestão do Risco – Pergunta 3

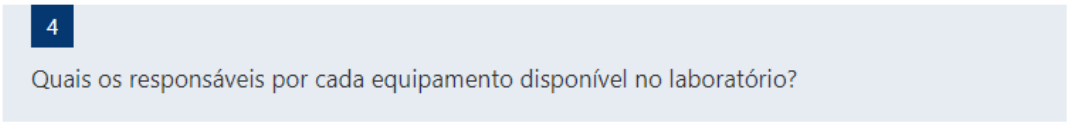


Figura 65 - Questionário Gestão do Risco – Pergunta 4

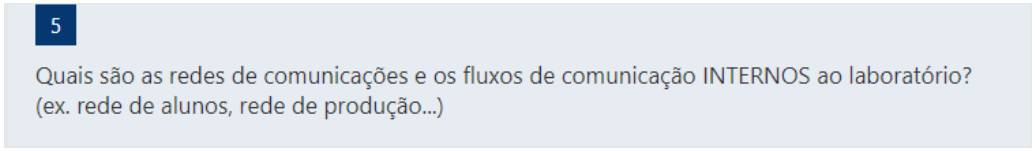


Figura 66 - Questionário Gestão do Risco – Pergunta 5

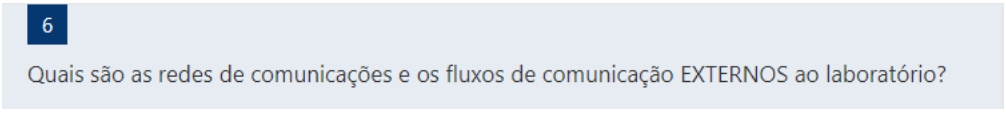


Figura 67 - Questionário Gestão do Risco – Pergunta 6

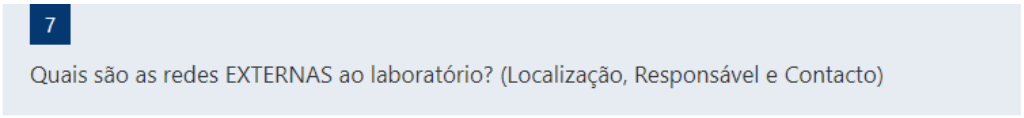


Figura 68 - Questionário Gestão do Risco – Pergunta 7

Figura 69 - Questionário Gestão do Risco – Pergunta 8

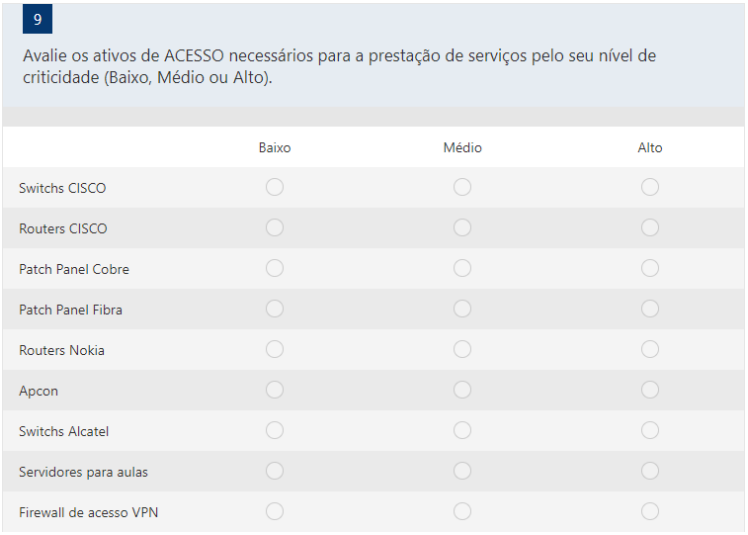


Figura 70 - Questionário Gestão do Risco – Pergunta 9

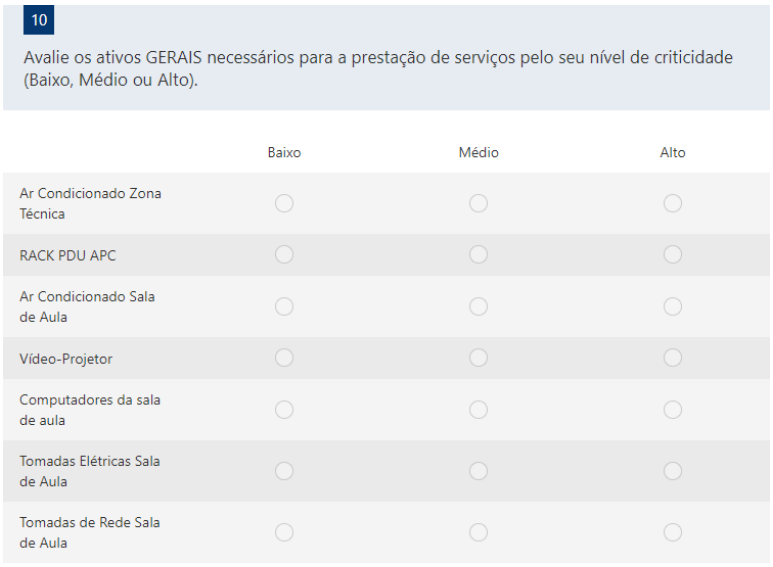


Figura 71 - Questionário Gestão do Risco – Pergunta 10

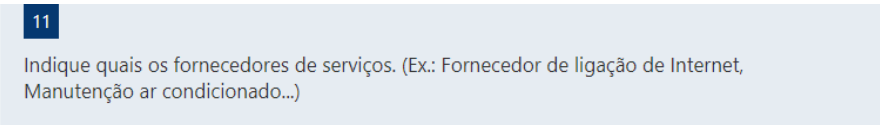


Figura 72 - Questionário Gestão do Risco – Pergunta 11

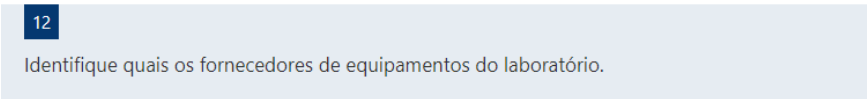


Figura 73 - Questionário Gestão do Risco – Pergunta 12

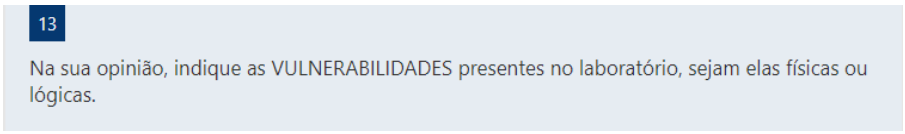


Figura 74 - Questionário Gestão do Risco – Pergunta 13

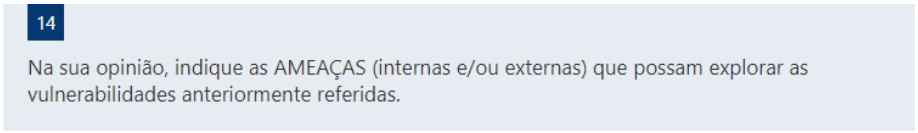


Figura 75 - Questionário Gestão do Risco – Pergunta 14

Figura 76 - Questionário Gestão do Risco – Pergunta 15

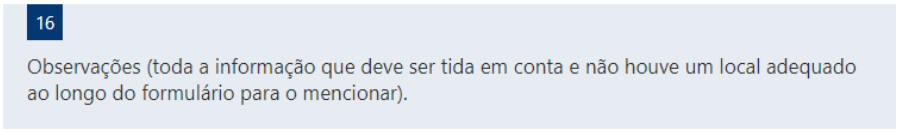


Figura 77 - Questionário Gestão do Risco – Pergunta 16

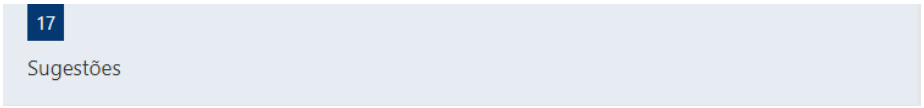


Figura 78 - Questionário Gestão do Risco – Pergunta 17

9.13 Anexo 13 – Relatório de Gestão de Risco do Laboratório de Redes e Sistemas Informáticos do ISMAI (Lab10)

Relatório de Gestão de Risco do Laboratório de Redes e Sistemas Informáticos do ISMAI (Lab10)

Maria João Abrantes Lage nº30415

Índice

Lista de Acrónimos

APD - Associação Porto Digital APD

CCTV - *Closed-circuit Television*

CD - *Continuous Delivery*

CI - *Continuous Integration*

CSIRT - *Computer Security Incident Response Team*

DLP - *Data Loss Prevention*

ENISA - *The European Union Agency for Cybersecurity*

GISI - Gabinete de Informática e Sistemas de Informação

IDS - *Intrusion Detection System*

IPS - *Intrusion Prevention System*

LDAP - *Lightweight Directory Access Protocol*

LE - *Law Enforcement*

NIST - *National Institute of Standards and Technology Interagency Report*

QNRCS - Quadro Nacional de Referência para a Cibersegurança

RACI - *Responsible, Accountable, Consulted e Informed*

RGPD – Regulamento Geral sobre a Proteção de Dados

Sistema AVAC – Sistema de Aquecimento, Ventilação e Ar Condicionado

VPN - *Virtual Private Network*

Introdução

Nos dias de hoje, segundo Paulsen, C. Toth, 2016, do *National Institute of Standards and Technology Interagency Report* (NIST), as empresas têm como principal valor a informação. Essa informação pode ser sobre funcionários, recursos, clientes e parceiros, entre outros. Segundo Office of the Law Revision Counsel of the U.S. House of Representatives., 1968, a segurança da informação tem como principal objetivo proteger os sistemas de informação contra o acesso não autorizado, o uso indevido, a divulgação, a modificação ou a destruição da informação, garantindo assim a integridade, confidencialidade e disponibilidade da mesma.

Com a evolução da tecnologia e o aumento do fluxo de informação, a informatização da mesma tornou-se uma prática quase obrigatória nas organizações. Com isso veio a necessidade do aumento de proteção da informação digital, e foi aí que a cibersegurança começou a ter um papel fundamental nas organizações.

Segundo Systems, 2015, Chung et al., 2014 e Paulsen, C. Toth, 2016, a cibersegurança é formalmente definida como meio de prevenção de danos, proteção e restauro de computadores, sistemas e serviços de comunicações eletrónicas, incluindo as informações nelas contidas, de forma a garantir a sua integridade, autenticidade, confidencialidade e disponibilidade.

O seguinte relatório tem como objetivo documentar o levantamento feito dos equipamentos e das vulnerabilidades do laboratório 10, tendo em conta as medidas homogénicas propostas pelo Quadro Nacional de Referência para a Cibersegurança (QNRCS). "*…o Centro Nacional de Cibersegurança reuniu o conjunto das melhores práticas num Quadro Nacional de Referência para a Cibersegurança, o qual permite às organizações reduzir o risco associado às ciberameaças…*" (Centro Nacional de Cibersegurança, 2019). Este relatório foi feito com a ajuda de um questionário apresentado aos docentes e monitores do laboratório 10.

Identificar

A primeira medida de proteção proposta tem como propósito ajudar a organização a compreender o seu contexto, "*… dos ativos que suportam os processos críticos da atividade da organização e os riscos associados relevantes. Esta compreensão permite que a organização consiga definir e priorizar os seus recursos e investimentos de acordo com os seus objetivos gerais e com a sua estratégia de gestão do risco.*" (Centro Nacional de Cibersegurança, 2019).

Esta medida é dividida em seis categorias (**ID.GA**, **ID.AO**, **ID.GV**, **ID.AR**, **IS.GR** e **ID.GL**) e cada categoria é divida entre duas a cinco subcategorias.

ID.GA – Gestão de Ativos

ID.GA-1 – Os dispositivos físicos, redes e sistemas de informação existentes na organização devem ser identificados

Na Figura 1 estão identificados os equipamentos, que, há data, estão presentes no laboratório 10. De forma a melhorar e cumprir o que é pedido nesta subcategoria ID.GA1, a nível dos dispositivos físicos e sistemas, a informação a acrescentar à tabela seria o **número de inventário** e o **número de série** do dispositivo. Juntamente com esta informação, aos dispositivos de rede deve ser acrescentada informação sobre o **endereço IP** e o **endereço de *hardware***. Deverá também ser devidamente identificado e documentado os responsáveis por cada dispositivo e sistemas, sendo necessário o seu **nome** e **contacto**. Por fim, a acrescentar à tabela apresentada na Figura 1, "*Os dispositivos físicos e sistemas devem ser classificados de acordo com a sua criticidade…*". (Centro Nacional de Cibersegurança, 2019)

Zona	Equipamento	Quantidade
Bastidor A	Switch Gestão Alcatel Gigabit 24 portas	2
	OLT	1
	ONT	5
Bastidor B	Router CISCO ISR1841	4
	Router CISCO ISR4221/K9	4
	Switch CISCO (dinâmicos)	8
	Firewall ASA 5506-x	4
	Switch Alcatel distribuição	1
	Patch Panel Cobre	1
	Patch Panel Fibra	1
Bastidor C	Router CISCO ISR1841	4
	Router CISCO ISR4221/K9	4
	Switch CISCO (dinâmicos)	8
	Firewall ASA 5506-x	4
	Switch Alcatel distribuição	2
Bastidor D	Patch Panel Cobre	1
	Patch Panel Fibra	1
	Router Nokia	8
	Apcon	1
	Switch CISCO 48 portas	1
	Switch Alcatel	1
	Switch Alcatel distribuição	1
	Switch Gestão Alcatel Gigabit 24 portas	2
	Firewall Cisco ASA5520-K8	1
Bastidor E	Patch Panel Cobre	1
	Patch Panel Fibra	1
	Switch Gestão CISCO Gigabit 24 portas	2
	Switch CISCO 24 portas	
	Servidores de virtualização	4
Sala Técnica	Ar-condicionado	2
	Tomadas	

Figura 1 – Lista de Equipamentos

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 1;
- COBIT 5 BAI09.01, BAI09.02;
- ISO/IEC 27001:2013 A.8.1.1, A.8.1.2;
- NIST SP 800-53 Rev. 4 CM-8, PM-5.

ID.GA-2 – As aplicações e plataformas de software que suportam os processos dos serviços críticos devem ser inventariadas

Com base no questionário mencionado na introdução, foram identificadas as seguintes aplicações/*software* presentes no laboratório 10:

- Plataforma de virtualização *Proxmox*;
- VPN-Lab10;
- EVE-NG;
- Software de gestão de credenciais (*TeamPass*);
- Software de gestão de identidades (LDAP);
- *Firmware* dos equipamentos.

Estas aplicações/*software* devem ser devidamente documentadas e inventariadas, devem ser identificados os **responsáveis** com o **nome** e **contacto** do mesmo, cada uma delas deve ser classificada pela sua **criticidade** para o laboratório 10 e, por fim, quando aplicável, deve ser identificado o tipo de contrato em vigor com o fornecedor da aplicação/*software*.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 2;
- COBIT 5 BAI09.01, BAI09.02, BAI09.05;
- ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1;
- NIST SP 800-53 Rev. 4 CM-8, PM-5.

ID.GA-3 – As redes e fluxos de dados devem ser mapeados

Na Figura 2 estão representadas as redes de comunicação internas presentes no laboratório 10. De forma a seguir o método aconselhado por esta subcategoria, é necessário,

no caso específico do laboratório 10, **criar o inventário os ativos** da rede de comunicação e **desenhar a topologia** da mesma.

Tipo de Rede	Endereço IP/Máscara de Rede	VLAN (x = não aplicável)
Produção/Gestão	192.168.200.240 255.255.255.0	41
Desenvolvimento	192.168.199.254 255.255.255.0	199
Servidores - Desenvolvimento	192.168.201.254 255.255.255.0	201
Servidores - Produção	192.168.202.254 255.255.255.0	202
PCs	192.168.203.254 255.255.255.0	203
Gestão de interfaces ILO	192.168.204.254 255.255.255.0	204
Interligação GISI	192.168.210.2 255.255.255.248	x
Internet	185.101.177.149 255.255.255.248	x
VPN Pool	172.16.10.0 255.255.255.0	x

Figura 2 - Redes de Comunicação Internas

Relativamente às redes de comunicação externas, existe a rede de interligação com a Associação Porto Digital (APD), uma interligação com o Gabinete de Informática e Sistemas de Informação (GISI) e, por fim, existe uma VPN de acesso remoto disponibilizada pela Maiêutica que permite a gestão remota do LAB10.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 12;
- COBIT 5 DSS05.02;
- ISO/IEC 27001:2013 A.13.2.1, A.13.2.2;
- NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8.

ID.AO – Ambiente da Organização

ID.AO-1 – O papel da organização na cadeia logística deve ser identificado e comunicado

De forma a documentar a cadeia logística, é necessário que o laboratório 10 consiga identificar e tipificar os seus fornecedores. Também devem ser adotadas medidas de gestão dos fornecedores, e definir critérios, procedimentos e comportamentos que devem ser adotados quando é celebrado um contrato.

Após ser celebrado um contrato, deve ser documentada a **identificação** do fornecedor, o **âmbito da relação** com esse fornecedor, a definição do serviço prestado (**essencial ou eventual**), e, por fim, o contacto do laboratório 10 que ficará responsável por responder pelo desempenho técnico e comportamentos do fornecedor.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05;
- ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2;
- NIST SP 800-53 Rev. 4 CP-2, SA-12.

ID.AO-4 – Os ativos críticos devem ser identificados e registados

As Figuras 3, 4 e 5 respondem a diferentes perguntas, mas todos com o mesmo objetivo: de entender, na opinião dos inquiridos, qual a criticidade de cada ativo necessário para a prestação de serviços ao qual o laboratório 10 se propõe.

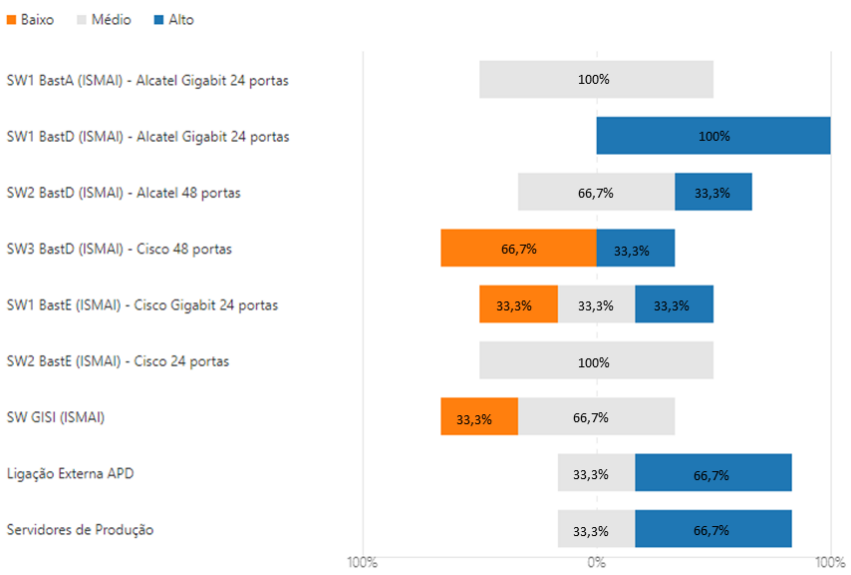


Figura 3 - Ativos de CORE e a sua criticidade

Na Figura 3, correspondente aos ativos de *CORE* da rede. Pode-se analisar que todos os equipamentos são analisados com criticidade de média a alta.

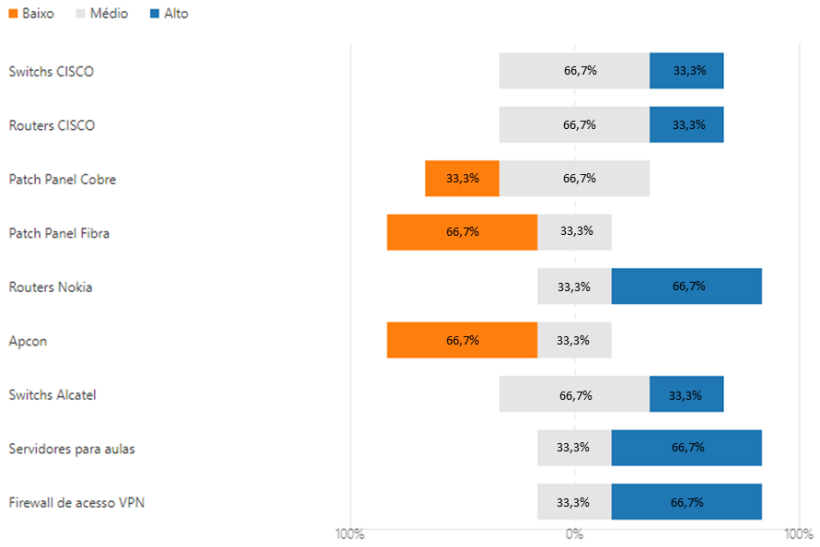


Figura 4 - Ativos de Acesso e sua criticidade

Na Figura 4 estão representados os ativos de acesso. Estes equipamentos são os ativos que serão utilizados no laboratório 10 para acesso à rede. Os *PatchPanel* (cobre e fibra) e o

APCON são os ativos que são classificados como baixo ou médio nível de criticidade, sendo que a média de criticidade dos ativos fica entre os níveis médio e alto.

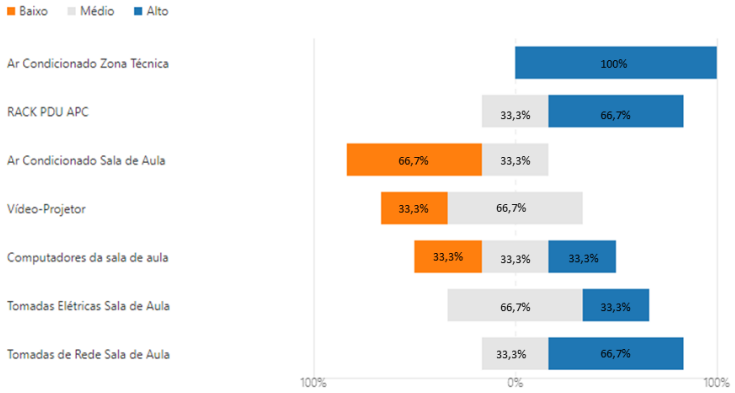


Figura 5 - Outros Ativos e sua criticidade

Por fim, na Figura 5, os inquiridos foram questionados sobre o nível de criticidade de alguns dos outros ativos presentes no laboratório 10. De salientar que a média do nível de criticidade varia entre o médio e alto. Através da análise das figuras, é possível concluir que o laboratório tem o mínimo de ativos necessários para o normal funcionamento do mesmo.

O QNRCS recomenda, nesta subcategoria, que sejam devidamente identificados todos os **ativos críticos** e, neste registo, devem ser incluídos todas as redes e sistemas que deem suporte aos serviços considerados críticos que necessitem de ser protegidos de falhas de energia ou outras anomalias, toda a cablagem elétrica e/ou redes de comunicações que necessitem de proteção contra danos e a monitorização das redes de modo a se conseguir efetuar previsões de necessidades futuras.

A identificação correta destes **ativos e das suas necessidades** vai permitir que possam ser asseguradas a capacidade e a redundância da rede em caso de falha. Essa redundância, segundo o Centro Nacional de Cibersegurança, 2019, pode ser obtida através de **UPS de suporte**, **ligações de comunicação redundantes**, **sistemas AVAC** e mapeamento dos pontos de rede.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 APO10.01, BAI04.02, BAI09.02;
- ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3;
- NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14.

ID.AO-5 – Os requisitos de resiliência necessários para suportar a prestação de serviços devem ser definidos

Aos inquiridos, utilizadores do laboratório 10, foi pedido que avaliassem qual o nível de criticidade em vinte cenários de risco apresentados. A Figura 6 representa as respostas dos inquiridos relativamente aos cenários apresentados e de que forma acham que pode afetar a prestação de serviços críticos.

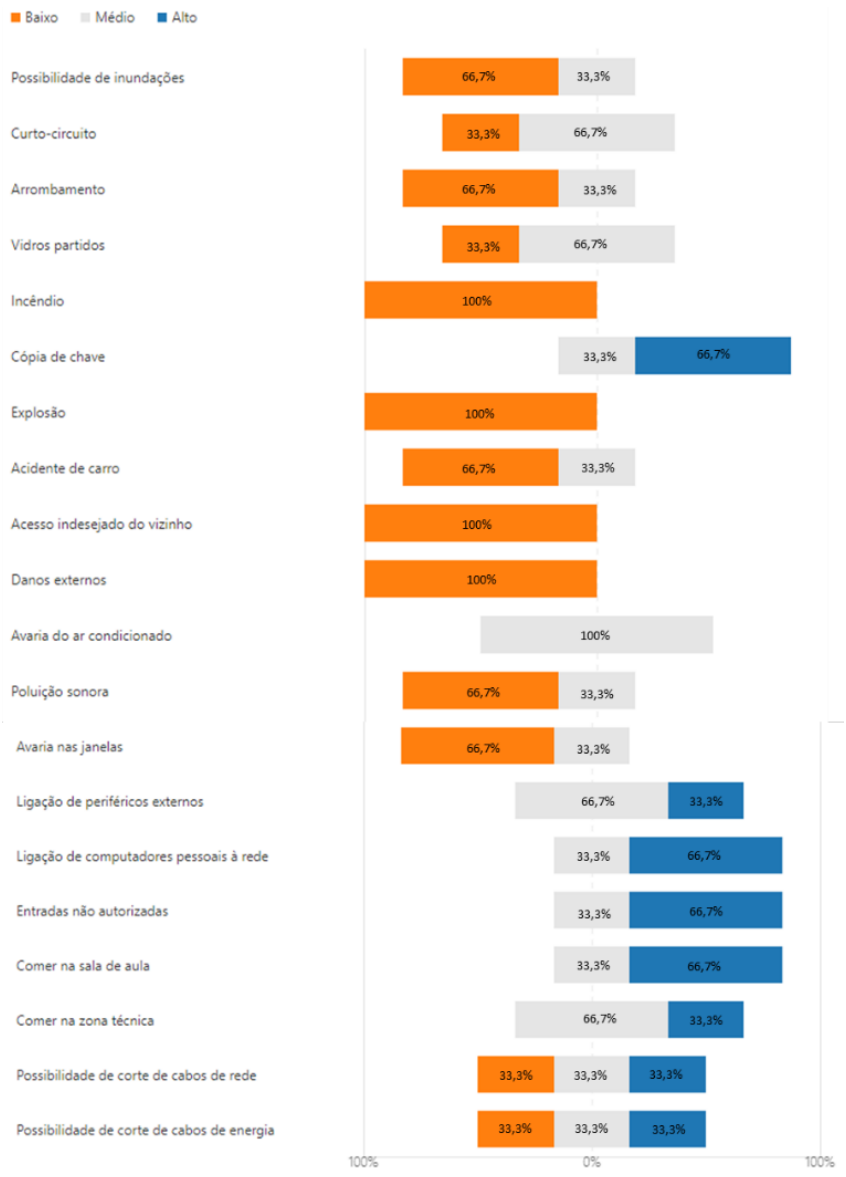


Figura 6 – Possíveis cenários e a sua criticidade

Este levantamento permite responder ao que a subcategoria descrita no QNRCS menciona: a **identificação de cenários de crise**. Após este passo, é necessário que seja definida uma **estratégia de recuperação** após desastres naturais e/ou ataques maliciosos. Por fim, deve ser **definido um plano de recuperação** dos serviços críticos e nesse plano

devem ser mencionados as **atividades**, **tempos** e **necessidades** de recuperação e os respetivos **testes de recuperação**.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 BAI03.02, DSS04.02;
- ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1;
- NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA-14.

ID.GV – Governação

ID.GV-1 – A política de segurança da informação deve ser definida e comunicada

A **política de segurança** deve ser devidamente **identificada**, justificando qual o motivo da sua definição. Este documento tem de ser formalmente aprovado pela gestão de topo da Maiêutica/laboratório 10. Após a criação deste documento, em formato digital, o mesmo deve ser publicado em plataformas de fácil acesso para que as partes interessadas possam ter conhecimento da política aplicada. Por fim, é aconselhado que seja confirmada a tomada de conhecimento da política por todas as partes interessadas.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 19;
- COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02;
- ISO/IEC 27001:2013 A.5.1.1;
- NIST SP 800-53 Rev. 4 -1 todos os controlos de segurança.

ID.GV-2 – Os requisitos legais e regulamentares para a cibersegurança devem ser cumpridos

No documento em que é descrita a **política de segurança da informação**, devem ser identificadas as conformidades legais nacionais e europeias (Assembleia da República, 2018b) (Comissão Europeia, 2016a).

Por fim, a definição de "*uma **política de privacidade** de acordo com a legislação nacional e europeia em vigor*". Para consolidar a aplicação destas medidas, devem ser feitos **relatórios de auditoria** que comprovem a aplicação das mesmas.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 19;
- COBIT 5 BAI02.01, MEA03.01, MEA03.04;
- ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5;
- NIST SP 800-53 Rev. 4 -1 todos os controlos de segurança.

ID.AR – Avaliação de Risco

ID.AR-1 – As vulnerabilidades dos ativos devem ser identificadas e documentadas

O processo de gestão de vulnerabilidades é uma das bases fundamentais da avaliação de risco. A gestão de vulnerabilidades consiste na **identificação de todas as vulnerabilidades** anteriormente não identificadas e/ou solucionadas. Após esta identificação, preferencialmente feita durante a análise de risco do laboratório 10, deve ser devidamente **definida e formalizada qual a estratégia a aplicar**.

No processo de análise de risco devem ser identificadas e tipificadas as vulnerabilidades de cada ativo que pode ser alvo de possíveis ameaças e, também, devem ser descritas quais as vulnerabilidades já identificadas, mas que ainda não foram solucionadas.

Na Figura 7 são apresentadas as respostas dadas pelos inquiridos ao que consideram ser as vulnerabilidades do laboratório 10, sendo:

- "Sala frágil, ao lado de uma via onde passam carros";
- "Passwords dos equipamentos de gestão fracas";
- "Falta de UPS";
- "Acesso à internet e à rede do GISI sem redundância";
- "Inexistência de soluções de backups";
- "Controlo de acesso à sala e ao DC [DataCenter] é pouco robusto";
- "Falta de uma plataforma para gestão de endereçamento IP";
- "Falta de uma plataforma de gestão e backup de configurações";
- "Falta de uma plataforma de monitorização da operacionalidade da rede e dos equipamentos da rede";
- "A inexistência de uma plataforma autenticação centralizada dificulta a gestão de utilizadores e a visibilidade sobre as ações dos mesmos";
- "Os alunos possuem um utilizador com privilégios de administração dos routers";
- "Não existe qualquer tipo de gestão dos acessos dos alunos à VPN do LAB10 (i.e. controlo de horário de acesso e acesso a recursos)".

ID ↑	Name	Responses
1	anonymous	Facil acesso ao espaço do laboratório. Sala frágil ao lado de uma via onde passam carros. Passwords dos equipamentos de gestão fracas.
2	anonymous	Falta de UPS, Acesso à internet e à rede do GISI sem redundância, Inexistência de solução de backups
3	anonymous	Controlo de acessos à sala e ao DC é pouco robusto; Falta de plataforma para gestão de endereçamento IP; Falta de plataforma de gestão e backup de configurações; Falta de plataforma de monitorização da operacionalidade da rede dos equipamentos da rede; A inixitência da uma plataforma de autenticação centralizada dificulta a gestão de utilizadores e a visibilidade sobre as ações dos mesmos; Os alunos possuem um utilizador com provilégios de administração dos routers. Não existe atualmente qualquer tipo de gestão dos acessos dos alunos à VPN do LAB10 (i.e. controlo de horário de acesso e acesso a recursos).

Figura 7 - Pergunta 13 – Na sua opinião, indique as vulnerabilidades presentes no laboratório, sejam elas físicas ou lógicas

Após análise das vulnerabilidades acima apresentadas foi concluído que a principal preocupação dos inquiridos é a segurança e o melhor funcionamento da sala técnica do laboratório 10 e dos equipamentos lá presentes. Esta preocupação deve-se a diversos fatores tais como a **falta de suporte a nível de eletricidade**, a **falta de redundância nas ligações com as redes externas**, a **falta de *backups* da informação** presente em toda a rede do laboratório, a **fácil acessibilidade por parte dos alunos à gestão** de alguns equipamentos, **não estar implementada uma plataforma de autenticação** pois os docentes também utilizam as mesmas credenciais para entrar em determinados equipamentos, a **falta de regularização de regras para a utilização da VPN** do laboratório e, por fim, a inexistência de um **controlo de acesso** mais robusto ao laboratório 10.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 4;
- COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02;
- ISO/IEC 27001:2013 A.12.6.1, A.18.2.3;

- NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5.

ID.AR-2 – A organização deve partilhar informações sobre ameaças de cibersegurança com grupos de interesse de especialidade

A **troca de informação e experiências** com "***grupos de interesse e especialistas técnicos*****"** (Centro Nacional de Cibersegurança, 2019) vai permitir a aprendizagem de **boas práticas** sobre a segurança da informação. Com a consulta de **fontes de informação da especialidade**, também será possível ter acesso a informação sobre **ameaças** de cibersegurança.

As **fontes de partilha de informação** poderão ser em **formato digital** e suscetíveis ao uso de interfaces aplicacionais e, por isso, é importante a criação de **mecanismos automáticos de recolha, tratamento e armazenamento** das fontes. Será importante a correlação destas fontes com a **gestão de eventos**.

Relativamente aos registos necessários, será importante elaborar um **registo** dos contactos com "***grupos de interesse***, ***listas de distribuição*** *e* ***especialistas técnicos*****"** (Centro Nacional de Cibersegurança, 2019) e um registo para a integração com **fontes de conhecimento externas**.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 4;
- COBIT 5 BAI08.01;
- ISO/IEC 27001:2013 A.6.1.4;
- NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16.

ID.AR-3 – As ameaças internas e externas devem ser identificadas e documentadas na metodologia de gestão de risco

Na Figura 8 são apresentadas as respostas dadas pelos inquiridos à questão "Na sua opinião, indique as AMEAÇAS (internas e/ou externas) que possam explorar as vulnerabilidades anteriormente referidas." (Mencionadas na Figura 7). De seguida será apresentado um resumo do que está demonstrado na Figura 8 relativamente a ameaças:

- "Alunos que queiram com intenção maliciosa estragar equipamentos ou mudar a topologia do laboratório";
- "Ar condicionado que possa avariar pois não existe monitorização sobre eles";
- "Alunos ou professores distraídos";
- "O facto de os alunos possuírem o login de *admin*, principalmente dos equipamentos Nokia 7750, pode levar a que os mesmos atuem de forma a impedir o acesso remoto aos mesmos (isto é, apagar o ficheiro *bof.cfg*)";
- "A concorrência de acesso a recursos é também um problema."

ID ↑	Name	Responses
1	anonymous	Alunos que queiram com intenção maliciosa estragar equipamentos ou mudar a topologia do laboratório, Ar condicionado que possa avariar pois não existe monitorização sobre eles. Alunos ou professores distraídos.
2	anonymous	O facto de os alunos possuirem o login de admin, principalmente nos equipamentos Nokia 7750, pode levar a que os mesmos atuem de forma a impedir o acesso remoto aos mesmos (isto é, apagar o ficheiro bof). Esta ameaça poderá ser mitigada com a introdução de um equipamento concentrador de interfaces de consola, ou com a criação de um utilizador com menos privilégios para os alunos. A concorrência de acesso a recursos é também um problema. Por exemplo, um alunos poderá aceder aos equipamentos por VPN ao mesmo tempo que estão a decorrer aulas laboratoriais.

Figura 8 - Pergunta 14 – Na sua opinião, indique as ameaças (internas e/ou externas) que possam explorar as vulnerabilidades anteriormente referidas.

As ameaças vão de encontro às vulnerabilidades identificadas e isso reforça a necessidade de atuação nas questões mencionadas na ID.AR-1, reforçando a ideia da necessidade de ter especial atenção às potenciais ameaças à sala técnica.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 4;
- COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04;
- ISO/IEC 27001:2013 Cláusula 6.1.2;
- NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16.

ID.AR-4 – A gestão do risco deve ser efetuada com base na análise de ameaças, vulnerabilidade, probabilidades e impactos

Na metodologia da gestão de risco do laboratório 10 deve ser **identificado os critérios** que apoiam a atribuição de uma probabilidade e de um impacto a cada um dos riscos. Estes critérios vão permitir que seja calculado o **nível de criticidade de cada um dos riscos**. De forma a identificar os riscos, devem ter tidas as em conta as **vulnerabilidades e as ameaças identificadas anteriormente** no documento (respetivamente ID.AR1 e IDAR3).

De forma a atribuir uma prioridade ao tratamento dos riscos identificados, é necessário ter em conta alguns fatores: o **impacto** do risco, a **probabilidade** de o risco ocorrer e a **relevância** do ativo para o laboratório 10.

O CNCS sugere uma fórmula que permite que o nível de risco possa ser mais objetivo: **IMPACTO x PROBABILIDADE x VALOR DO ATIVO**. O valor do ativo, tal como mencionado em cima, apenas deve utilizado na fórmula se for aplicável.

Relativamente aos intervalos dos níveis de impacto e de probabilidade, os mesmos podem ser definidos e estipulados pela Maiêutica. No QNRCS é apresentado um exemplo

em que o João utilizou a matriz na metodologia do risco definida pela Organização. Para a avaliação do **impacto** estavam definidos os seguintes níveis: "***1 – Pequeno, 2 – Moderado, 3 – Elevado, 4 – Catastrófico*****"** . A nível da **probabilidade**, foi definido pela Organização do João que a avaliação da probabilidade de o risco acontecer poderá ser: "***1 – Improvável, 2 – Provável, 3 – Muito Provável, 4 – Quase Certa*****"**. Juntamente com estes níveis, devem ser definidos os critérios de identificação dos níveis de risco (resultado da fórmula acima apresentada). No Organização do João foram definidos os seguintes intervalos de conclusão: "***[1,2] - Nível Baixo, [3 a 6] - Nível Médio, [8 a 12] - Alto, [16] - Muito Alto"***. (Centro Nacional de Cibersegurança, 2019)

Em suma, é importante que a Maiêutica defina com precisão quais os níveis a adotar em cada um dos critérios de avaliação de um determinado risco. Esta avaliação é extremamente importante de forma a entender o que realmente é um risco para o laboratório 10 e de que forma se pode minimizar ou até mesmo ultrapassar esse risco.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 4;
- COBIT 5 APO12.02;
- ISO/IEC 27001:2013 A.12.6.1;
- NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16.

ID.AR-5 – A organização deve garantir que as respostas aos riscos são identificadas e priorizadas

Após o cálculo dos riscos, deve ser definida uma **estratégia de priorização do tratamento** destes mesmos riscos. Esta prioridade deve ser definida com base no **nível de risco** calculado anteriormente e a **criticidade do ativo** para o laboratório 10.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 4;
- COBIT 5 APO12.05, APO13.02;
- ISO/IEC 27001:2013 Cláusula 6.1.3;
- NIST SP 800-53 Rev. 4 PM-4, PM-9.

ID.GR – Estratégia de Gestão de Risco

ID.GR-1 – A organização deve definir um processo de gestão do risco

A gestão dos riscos e o seu processo exige que a Maiêutica, com ajuda de sistemas de informação orientados para a gestão do risco, defina uma **estratégia** de forma consistente com a **utilização e operação das redes e sistemas de informação** do laboratório 10 e que esta seja consistente e comunicada a todos os intervenientes do laboratório, que sejam nomeadas pessoas para assumirem as **responsabilidades** pelo **processo de gestão do risco** e pelo **tratamento do risco**.

O processo deve ter em consideração os **riscos operacionais e organizacionais**. Deve ser do conhecimento de todos os intervenientes qual a **estratégia de tolerância ao risco** definida e aceite, quais os **métodos** de **definição**, **avaliação** e **tratamento** dos riscos e quais os métodos de **controlo** da **evolução** dos **riscos**.

"*A metodologia de gestão do risco a escolher poderá ser baseada na norma ISO/IEC 27005 que orienta as organizações no processo de definição e identificação de regras e práticas de gestão dos riscos de segurança da informação*". (Centro Nacional de Cibersegurança, 2019)

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 4;
- COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02;
- ISO/IEC 27001:2013 Cláusula 6.1.3, Cláusula 8.3, Cláusula 9.3;

- NIST SP 800-53 Rev. 4 PM-9.

ID.GR-2 – A organização deve determinar e identificar a sua tolerância ao risco

Na **metodologia de gestão de risco**, devidamente documentada, deve ser definida a **estratégia de tratamento de risco**. Essa estratégia deve ter em consideração os **níveis dos riscos existentes** e qual a **tolerância** da Maiêutica/laboratório 10 aos mesmos. Esta estratégia deve gerar um processo de aprovação por parte da gestão de topo.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 APO12.06;
- ISO/IEC 27001:2013 Cláusula 6.1.3, Cláusula 8.3;
- NIST SP 800-53 Rev. 4 PM-9.

ID.GR-3 – A organização deve definir a sua estratégia de tratamento do risco

Relativamente ao tratamento do risco, deve ser definida qual a estratégia a usar de forma a ser aplicado o tratamento do risco aos ativos críticos, identificados anteriormente. As possíveis **respostas para o tratamento do risco** devem ser as seguintes:

- **evitar** o risco: definir uma ou várias regras de forma a diminuir a probabilidade e/ou o impacto de um risco, tendo em conta que quanto mais próxima de zero, mais difícil de ocorrer e/ou de o eliminar na totalidade;
- **aceitar** o risco: se esta for a decisão tomada para um determinado evento, a mesma deve ser formalmente comunicada pela Maiêutica;

- **mitigar** o risco: a probabilidade e/ou impacto de um determinado evento adverso pode ser reduzida para limites suportáveis através da implementação de métodos de controlo; e, por fim;
- **transferir** o risco: transferência do impacto de uma ameaça, total ou parcialmente, para terceiros.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 APO12.02;
- ISO/IEC 27001:2013 Cláusula 6.1.3, Cláusula 8.32;
- NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM-11.

ID.GL – Gestão do Risco da Cadeia Logística

ID.GL-1 – A organização deve definir, avaliar e gerir processos de gestão do risco da cadeia logística

A Maiêutica deve efetuar uma **análise** às **partes interessadas** que pertencem à **cadeia logística do laboratório 10**. A análise deve ser feita com a metodologia de análise e gestão do risco que foi definida internamente.

A **política de gestão de fornecedores**, falada na subcategoria ID.GL2, para além da informação dos mesmos, deve identificar os **responsáveis internos** pela análise de risco e qual a **periocidade** dessas mesmas análises.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 4;
- COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02;

- ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2;
- NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9.

ID.GL-2 – A organização deve avaliar o risco da cadeira logística de cibersegurança

Nesta subcategoria é pedido que sejam **identificados**, **prioritizados** e **avaliados** os **fornecedores de redes e sistemas de informação** e os **componentes e serviços de cibersegurança**. Esta ação terá de seguir "*um processo de avaliação do risco da cadeia logística de cibersegurança*" (Centro Nacional de Cibersegurança, 2019).

A categorização dos fornecedores deve ser feita tendo em conta: "*a **exposição da informação aos fornecedores**, o **impacto na cadeia logística** e o **tipo de bens e serviços fornecidos***" (Centro Nacional de Cibersegurança, 2019) pelo laboratório 10.

A política de gestão dos fornecedores deve conter as seguintes informações: **nome** do fornecedor, o **tipo** de fornecedor, a **criticidade** para a prestação dos serviços críticos, e por fim, relativamente ao **nível de exposição**, a confidencialidade, integridade e disponibilidade.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03;
- ISO/IEC 27001:2013 A.15.2.1, A.15.2.2;
- NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9.

ID.GL-3 – Os contratos com fornecedores devem respeitar o plano de gestão do risco para a cadeia logística

Os **contratos** com os fornecedores são também importantes para a **definir** e **garantir** que todos os **objetivos da política de segurança da informação** são cumpridos, tal como o plano de gestão do risco para a cadeia logística.

A **política de gestão de fornecedores** tem como obrigatoriedade conter: **cláusulas de confidencialidade nos contratos com os fornecedores** e **acordos de não divulgação com os mesmos e os seus colaboradores**. Este acordo deve garantir a confidencialidade sobre o tratamento da informação relativa à Maiêutica e ao laboratório 10, aos utilizadores do mesmo e aos restantes fornecedores.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05;
- ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3;
- NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9.

ID.GL-4 – Os fornecedores devem ser periodicamente avaliados

Os fornecedores devem ser **regularmente avaliados** com o uso de **auditorias**, **resultados de testes** ou outros métodos de forma a garantir que estão a ser cumpridas obrigações estipuladas nos contratos. Com isto, devem ser criados mecanismos de **medição da qualidade do serviço prestado** ou do produto fornecido pelos fornecedores.

Na política de gestão dos fornecedores, deve ser identificado: o **plano de auditoria** a aplicar, os métodos e os testes da mesma e o processo de **monitorização e melhoria** constante dos serviços prestados/produto fornecido. Estes pontos devem ser identificados com base na categorização que foi atribuída aos fornecedores. A categorização, proposta no ID.GL3, deve ser feita com base no nível de **exposição da informação** do laboratório 10 aos fornecedores.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05;
- ISO/IEC 27001:2013 A.15.2.1, A.15.2.2;
- NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12.

ID.GL-5 – O plano de resposta e recuperação de desastre deve ser exercitado com o acompanhamento de fornecedores

A Maiêutica deve identificar quais os **fornecedores** que têm de **participar no plano de recuperação e resposta**. Na lista dos fornecedores devem indicar se aquele fornecedor participa ou não no plano de resposta e/ou de recuperação. Se sim deve ser definido qual o plano a ele associado e deve ser destacado para participar nos testes e exercícios planeados.

Todos os resultados dos testes de recuperação a um desastre devem ser identificados num documento, tal como o registo e identificação dos fornecedores.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 19, 20;
- COBIT 5 DSS04.04;
- ISO/IEC 27001:2013 A.17.1.3;
- NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9.

Proteger

A medida de segurança Proteger tem como objetivo a criação de "*medidas orientadas à proteção da organização nas suas três dimensões: Pessoas, Processos e Tecnologia*" (Centro Nacional de Cibersegurança, 2019).

Esta medida de segurança é constituída por seis categorias (**PR.GA**, **PR.FC**, **PR.SD**, **PR.PI**, **PR.MA** e **PR.TP**) e várias subcategorias.

PR.GA - Gestão de Identidades, Autenticação e Controlo de Acessos

PR.GA-1 - O ciclo de vida de gestão de identidades deve ser definido

Nesta subcategoria é sugerido que se garanta que os **dados de identificação** e as **credenciais de acesso** às redes e sistemas de informação sejam "***emitidas, geridas, verificadas, revogadas*** *e* ***auditadas***" (Centro Nacional de Cibersegurança, 2019) em conformidade com os processos já definidos.

A Maiêutica deve "***criar***, ***disseminar***, ***rever*** *e* ***atualizar*** *o* ***processo de gestão de acessos a ativos***" (Centro Nacional de Cibersegurança, 2019) do laboratório 10, os perfis funcionais e acessos associados e os serviços de autenticação.

É recomendado a utilização de um **sistema de informação para a gestão de identidades e acesso**. Nesse sistema devem ser identificados os **tipos de sessões** existentes, definidas **regras e condições** para atribuição de **grupos e perfis** e definidos os **utilizadores que poderão ter acesso** a um determinado sistema de informação.

Nos sistemas também devem ser definidos os parâmetros necessários para a **atribuição de cada acesso**, a **criação**, **ativação**, **inativação**, **modificação** e **remoção** de **contas.** Também será necessário a notificação dos responsáveis do laboratório, por parte da Maiêutica, no caso de um acesso se tornar obsoleto, um utilizador ser reenquadrado numa nova função, quando o utilizador cessa relação institucional e quando se verifique necessário a alteração do perfil de um utilizador.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 1, 5, 15, 16;
- COBIT 5 DSS05.04, DSS06.03;
- ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3;
- NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11.

PR.GA-2 - Devem existir controlos de acesso físico às redes e sistemas de informação

A Maiêutica deve **proteger** e **gerir** o **acesso físico ao laboratório 10**. O controlo de acesso deve ser baseado em "***cartões magnéticos*** *(ou outro método de autenticação equivalente)* " e deve existir a "***integração do sistema de acessos*** *com o sistema de gestão de identidades*" de forma a parametrizar o acesso aos espaços físicos e uma validação central. O registo de **entradas e saídas de visitantes externos** deve conter dados como o **Nome**, **Empresa**, data/hora de **entrada**, data/hora de **saída**, o **responsável interno** pelo acompanhamento e o **motivo** da visita. (Centro Nacional de Cibersegurança, 2019)

A nível processual, deve ser **criada** e **mantida** uma **lista** com as pessoas com acessos autorizados ao laboratório 10 e a emissão de **credenciais de autorização** específicas. Esta lista deve ser revista e aprovada sempre que for necessário ou sempre que atingir um determinado intervalo de tempo desde a última avaliação, sendo este definido previamente.

O controlo de acesso ao laboratório 10 pode incluir um **controlo de identidade** dos alunos, docentes ou outro pessoal autorizado, um **registo** de auditoria na **passagem para a sala técnica** e a garantia de **acompanhamento interno** a visitantes.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 DSS01.04, DSS05.05;
- ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8;
- NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8.

PR.GA-3 - A organização deve gerir os seus acessos remotos

A Maiêutica deve "***documentar***, ***gerir*** *e* ***controlar*** *os* ***acessos remotos***" ao laboratório 10. "*São considerados acessos remotos, todos os acessos feitos às redes e sistemas de informação por colaboradores que comuniquem através de redes de comunicações externas à organização*" (Centro Nacional de Cibersegurança, 2019).

A implementação processual passa por a Maiêutica documentar uma **política de acessos remotos** ao laboratório 10, uma **política de teletrabalho** (se aplicável), **autorizar** formalmente os **acessos** e **definir** e **garantir** que são cumpridos os **requisitos** para os acessos ao laboratório 10.

Para além do documento em que estão descritas as políticas necessárias ao acesso remoto, deve existir uma solução tecnológica que permita o acesso remoto cifrado/seguro ao laboratório 10.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 12;
- COBIT 5 APO13.01, DSS01.04, DSS05.03;
- ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1;
- NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15.

PR.GA-4 - A organização deve aplicar na gestão de acessos, os princípios do menor privilégio e da segregação de funções

As **permissões** e as **autorizações** devem ser geridas com base na função do utilizador do laboratório 10. Por **menor privilégio** entende-se "*que a concessão de acessos às redes e sistemas de informação da organização aos colaboradores devem ser as estritamente necessárias para o correto desempenho das suas funções.*" (Centro Nacional de Cibersegurança, 2019). Relativamente à **segregação de funções**, "*a prática da divisão do conhecimento e de privilégios entre múltiplos indivíduos, de forma a que um processo em particular não possa ser executado ou controlado por apenas um deles*." (Centro Nacional de Cibersegurança, 2019).

A **segregação de funções** é uma medida aconselhada pois, existindo diversas pessoas envolvidas, existe mais probabilidade de serem detetadas e reportadas as possíveis transgressões. Segundo o QNRCS, este princípio pode ser aplicado com um dos seguintes tipos de processos:

"*1) Sequenciais: Quando as atividades podem ser executadas em tarefas sequenciais e por pessoas diferentes (por exemplo: na atribuição de acessos, uma pessoa solicita, outra aprova e uma terceira atribui os acessos);*

2) Quórum: Quando as atividades requerem um quórum mínimo de aprovações para poderem ser executadas (por exemplo: A recuperação de uma chave de cifra, onde é requerida a presença de dois ou mais administradores de sistemas);

3) Geoespacial: Quando as atividades podem ser divididas em tarefas que são realizadas em locais diferentes (por exemplo: Gestão de sistemas de informação cujas tarefas são efetuadas por colaboradores sediados em diferentes zonas geográficas)." (Centro Nacional de Cibersegurança, 2019)

A Maiêutica deve definir um **mapa de funções** adequado a cada perfil e a cada acesso, definir "*um processo formal para a gestão do ciclo de vida de acessos, praticar os princípios de menor privilégio*" e, por fim, utilizar a segregação de funções. (Centro Nacional de Cibersegurança, 2019)

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 3, 5, 12, 14, 15, 16, 18;
- COBIT 5 DSS05.04;
- ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5;
- NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24.

PR.GA-5 - A organização deve proteger a integridade das redes de comunicações

A rede de comunicações do laboratório 10 deve ser ajustada de forma a que não lhe seja possível aceder a partir de qualquer ponto. Para melhorar a **proteção** da mesma, devem ser criados **limites de segurança**, suportados por equipamentos como ***routers***, ***gateways***, ***firewalls***, entre outros, que permitam garantir essa mesma proteção.

A **segregação** e segmentação da rede de comunicações do laboratório 10 permitirá manter a **integridade** da mesma. Estas ações devem seguir políticas, devidamente documentadas, onde também estarão descritas as **autorizações necessárias** para a inserção de novos fluxos de informação.

No contexto deste documento, a **segregação das redes de comunicação** vai permitir a criação de zonas. A essas zonas serão atribuídas sub-redes, funcionalidades e regras de fluxos de comunicação. Esta segregação deverá seguir uma norma previamente definida.

A norma deverá contemplar quais as **sub-redes** definidas, as **funcionalidades** atribuídas a cada zona e quais as respetivas **regras de fluxos de comunicação** (na própria zona ou entre zonas). Relativamente aos fluxos de comunicação, deverão existir procedimentos de **revisão periódica das regras**, sendo o período temporal definido pela instituição, e a **alteração** dessas mesmas regras.

As **funções de gestão dos fluxos** de comunicações deverão estar devidamente segregadas. A **política de transferência de informação** tem de ser previamente definida

com a garantia do uso de uma cifra na comunicação. É importante que também sejam criadas **regras de utilização e acesso** às redes de comunicações.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 9, 14, 15, 18;
- COBIT 5 DSS01.05, DSS05.02;
- ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3;
- NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7.

PR.GA-6 – A organização deve verificar a identidade dos colaboradores e vinculá-las às respetivas credenciais

A instituição deve **rever** a **identidade dos colaboradores** e as suas **credenciais** sempre que for necessário. Essa verificação vai permitir confirmar que os acessos autorizados são realmente feitos pelo colaborador indicado e não por outras pessoas.

Previamente, deve ser definido e formalizado um processo para o **registo de novos colaboradores** (utilizador único e nominal), para o **cancelamento** de registos de ex-colaboradores e para a gestão de acessos.

Neste sentido devem ser feitos registos das **verificações dos antecedentes** dos colaboradores e essa verificação deve ser feita conforme a lei (RGPD - (Comissão Europeia, 2016b)) e tendo sempre em conta a função do mesmo e, por fim, devem ser documentados todos os processos formais mencionados anteriormente.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 16;
- COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03;
- ISO/IEC 27001:2013, A.7.1.1, A.9.2.1;

- NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3.

PR.GA-7 – Devem ser definidos mecanismos de autenticação de utilizadores, dispositivos, e outros ativos de sistemas de informação

A **autenticação de utilizadores**, **dipositivos** ou **ativos** deve ser feita com base em **mecanismos**, previamente definidos, que tenham como objetivo a **manutenção da integridade e da confidencialidade da informação**.

Para cumprir estes requisitos será necessário proceder à cr**iação e à manutenção de políticas de gestão de palavras-passe** e de **gestão de acessos**, que devem ser devidamente documentadas. E nas **redes/sistemas de informação mais críticos**, devem ser aplicados **múltiplos fatores de autenticação**, onde se deve fazer **auditorias** e o **registo das mesmas**.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 1, 12, 15, 16;
- COBIT 5 DSS05.04, DSS05.10, DSS06.10;
- ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4;
- NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11.

PR.FC - Formação e Sensibilização

PR.FC-1 - Os colaboradores devem ter formação em segurança da informação

A Maiêutica deverá definir e documentar um **plano de ações de formação** sobre a **segurança** da informação. As ações de formação devem ser direcionadas aos colaboradores e às partes interessadas.

No contexto em causa é importante ser tida em conta, igualmente, a s**egurança física**. Esta segurança física determina que **colaboradores podem circular e/ou estar perto do laboratório 10 e saber o que fazer no caso de ser detetada uma anomalia no laboratório**. A Maiêutica deverá definir um plano de ações de formação para a segurança física, sendo que este plano terá de ser de forma mais personalizada. Estas ações de formação deverão ser destinadas a um determinado número de pessoas que esteja responsável pelo corrente funcionamento e segurança das instalações da instituição.

Para garantir a **implementação** deste plano por parte dos membros mencionados anteriormente, é importante a **definição e registo** de quais os **processos e procedimentos** a serem adotados para a melhor implementação do mesmo.

Para qualquer um dos planos elaborados deverão ser feitos **registos das ações de formação** contendo os **conteúdos programáticos**, as **presenças** dos colaboradores e as provas que permitem a **verificação da aprendizagem**.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 17, 18;
- COBIT 5 APO07.03, BAI05.07;
- ISO/IEC 27001:2013 A.7.2.2, A.12.2.1;
- NIST SP 800-53 Rev. 4 AT-2, PM-13.

PR.FC-2 - Os utilizadores com acesso privilegiado devem compreender quais são os seus papéis e responsabilidades

As **ações de formação** aos **colaboradores** com **acessos privilegiados** às redes e sistemas de informação do laboratório 10 vão permitir que os mesmos tenham conhecimento sobre as suas **funções**, **papéis** e **responsabilidades**. Os conteúdos programáticos deverão ser adequados ao objetivo da formação e aos colaboradores que farão parte da mesma, que foram definidos anteriormente.

As ações de formação devem ser executadas antes dos colaboradores iniciarem as suas funções. No contexto em causa, as ações de formação deverão ser dadas quando os planos de ações de formação forem implementados, isto porque a maioria dos colaboradores já trabalha na instituição.

Deverão existir **novas ações de formação** sempre que exista **alterações** nos acessos atribuídos e numa **periocidade** definida pela instituição.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 5, 17, 18;
- COBIT 5 APO07.02, DSS05.04, DSS06.03;
- ISO/IEC 27001:2013 A.6.1.1, A.7.2.2;
- NIST SP 800-53 Rev. 4 AT-3, PM-13.

PR.FC-3 - As partes interessadas externas devem compreender quais são os seus papéis e responsabilidades

Os **alunos, docentes** e **fornecedores** (partes externas) também devem ter conhecimento dos **requisitos mínimos de segurança**, dos seus **papéis/funções** e **responsabilidades** no sistema de segurança do laboratório 10, aumentado, assim, o nível de segurança do mesmo. Estes requisitos mínimos deverão ser devidamente documentados e

partilhados com os alunos, docentes e fornecedores através de **ações de sensibilização**, durante as respetivas aulas e, possivelmente, através do uso de documentação pública afixada no laboratório 10.

Estas ações de sensibilização devem originar relatórios com a informação das mesmas e relatórios de auditorias que comprovem que os intervenientes estão a cumprir os requisitos previamente definidos.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 17;
- COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05;
- ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2;
- NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16.

PR.FC-4 - A gestão de topo deve compreender as suas funções e responsabilidades

A **gestão de topo** também deve estar integrada no processo de **compreensão da segurança da informação** (cibersegurança) e **física** do laboratório 10. Deverão ser igualmente definidos quais os **papéis** e **responsabilidades** da gestão de topo e também deverá participar nas **ações de formação** sobre a segurança.

Juntamente com os registos das ações de formação, também deve ser feita a **matriz RACI**[1] relativa à envolvência da gestão de topo no processo de segurança.

[1] Matriz RACI – Matriz de Responsabilidades (Khan & Quraishi, 2014)

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 17, 19;
- COBIT 5 EDM01.01, APO01.02, APO07.03;
- ISO/IEC 27001:2013 A.6.1.1, A.7.2.2;
- NIST SP 800-53 Rev. 4 AT-3, PM-13.

PR.SD - Segurança de Dados

PR.SD-1 - A organização deve proteger os dados armazenados

As **redes/sistemas de informação** presentes no laboratório 10 devem garantir a **confidencialidade** e a **integridade** da **informação** lá armazenada. Para garantir essa proteção, devem ser criados **serviços de cifra**, **bases de dados**, **cópias de segurança** e será necessário efetuar uma **validação criptográfica** dos dados armazenados. Os dados devem ser armazenados de acordo com a **classificação** atribuída a nível da confidencialidade necessária para os mesmos. Devem existir regras de armazenamento de documentos nos diversos tipos de dispositivos do laboratório 10 e deve ser criada uma política de cifra de informação em que a mesma deve ter em conta a proteção de dados armazenados com base na sua localização e classificação.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 13, 14;
- COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06;
- ISO/IEC 27001:2013 A.8.2.3;
- NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28.

PR.SD-2 - A organização deve proteger os dados em circulação

Juntamente com o ponto anterior, também é importante **proteger** a **integridade** e **confidencialidade** da informação que **circula na rede do laboratório 10**. Deve ser tida em conta tanto a rede interna como a rede externa.

O transporte da informação deve ser feito de forma segura, tendo como base as regras previamente definidas de **classificação da informação. A política de cifra** que deve ser aplicada deverá contemplar a proteção da confidencialidade e integridade da informação que circula nas redes do laboratório 10.

No caso de não ser possível garantir o **controlo de segurança mínimo**, devem ser implementados controlos compensatórios, não sendo isso possível a Maiêutica, juntamente com os responsáveis pelo laboratório, deve aceitar o risco e/ou o transferir para um fornecedor.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 13, 14;
- COBIT 5 APO01.06, DSS05.02, DSS06.06;
- ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3;
- NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12.

PR.SD-3 - A organização deve gerir formalmente os ativos durante os procedimentos de remoção, transferência e aprovisionamento dos mesmos

De forma a melhorar a segurança do laboratório 10, é necessário serem criados procedimentos de **autorização**, **monitorização**, **registo** e **aprovisionamento** das redes e sistemas de informação e dos **ativos** que entram ou saiam do laboratório 10. Também é importante serem criados processos de gestão do ciclo de vida dos ativos lá presentes.

Relativamente à informação/dados, quando estes não forem necessários para o laboratório 10 e para a Maiêutica, devem ser seguidos os procedimentos que indicam regras de remoção ou transferência dos dados em suporte físico amovível. Estas regras/mecanismos devem ser definidas com base na classificação de segurança dada a essa informação.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 1;
- COBIT 5 BAI09.03;
- ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7;
- NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16.

PR.SD-4 - A organização deve providenciar a capacidade adequada para garantir a disponibilidade das redes e dos sistemas de informação

Nesta subcategoria devem ser criados **procedimentos para medir a capacidade** das redes e dos sistemas de informação. A monitorização deve ser feita à **capacidade de armazenamento**, à **capacidade de memória** e à **largura de banda e latência** das redes. Esta monitorização deve permitir que sejam enviados **alertas** quando a capacidade atinge valores previamente definidos como críticos. Durante todo este processo é necessário realizar previsões relativamente a necessidades futuras, podendo estas ser posteriormente implementadas.

Por fim, é necessário, para completar este mecanismo, a implementação de redundância nas redes e sistemas de informação que suportem os serviços críticos do laboratório 10.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 1, 2, 13;

- COBIT 5 APO13.01, BAI04.04;
- ISO/IEC 27001:2013 A.12.1.3, A.17.2.1;
- NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5.

PR.SD-5 - A organização deve implementar proteções que evitem exfiltração de informação

Os **controlos de segurança** nas **delimitações** das instalações/redes e sistemas de informação do laboratório 10 são um passo fundamental para a **deteção**, e até **impedimento**, de **exfiltração** não autorizada da informação. É sugerida a implementação de sistemas de prevenção de perda de informação (DLP).

Para além deste sistema, devem ser adotadas medidas como a "***obrigatoriedade de usar formatos e protocolos*** *previamente definidos, monitorização para esteganografia*, ***restringir o uso de interfaces externas*** *de rede*", efetuar **análises ao tráfego** de forma a detetar desvios e, por fim, a criação de procedimentos que possam ser correspondentes com as regras de classificação da informação. (Centro Nacional de Cibersegurança, 2019)

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 13;
- COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02;
- ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4,A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3;
- NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI- 4.

PR.SD-6 - A organização deve utilizar mecanismos de verificação para confirmar a integridade de *software*, *firmware* e dados

De forma a serem detetadas manipulações não autorizadas e/ou erros de má utilização, devem ser criados **mecanismos de controlo de qualidade** que verificam a integridade dos *software*/*firmware*. Devem ser feitos **testes estáticos, dinâmicos e interativos** às redes e sistemas de informação do laboratório 10 e devem ser definidos mecanismos de verificação de integridade da informação.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 2, 3;
- COBIT 5 APO01.06, BAI06.01, DSS06.02;
- ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4;
- NIST SP 800-53 Rev. 4 SC-16, SI-7.

PR.SD-7 - Os ambientes de desenvolvimentos e de teste devem ser separados de ambientes de produção

A instituição deve garantir a **separação das redes e dos sistemas de informação** tanto de forma **física** como **lógica**, com base nas funções de cada uma. A nível de **ambientes de desenvolvimento e testes** e a nível de **ambientes de produção**, os mesmos devem estar **separados**, tal como os acessos a cada um associado e aos dados que neles circulam. Para cumprir esta implementação, deverão ser criadas **zonas de segurança** das redes de comunicações, separação física ou lógica dos ambientes e tornar anónimos os dados de produção para ambientes de teste.

Como complemento às ações executadas anteriormente, é importante a **criação**, **divulgação** e **atualização** de uma **política de desenvolvimento seguro de *software*** (**PR.PI-2**), a aplicação de **proteção aos ambientes de produção** de eventos não previstos originados por atividades de desenvolvimentos/testes, a **gestão de configurações** em cada ambiente de forma independente e adequada, garantindo a estabilidade na produção e a flexibilidade no desenvolvimento, a **anonimização dos dados de produção** antes da sua cópia para ambientes de desenvolvimento/teste e, por fim, a garantia que a colocação de **novas versões de *software*** em produção sejam geridas por processos de gestão de versões e alterações.

Os documentos de suporte deverão ser relativos ao desenvolvimento seguro de *software* e aos processos de gestão de alterações e versões.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 18, 20;
- COBIT 5 BAI03.08, BAI07.04;
- ISO/IEC 27001:2013 A.12.1.4;
- NIST SP 800-53 Rev. 4 CM-2.

PR.SD-8 - A organização deve implementar mecanismos de validação e verificação de integridade do hardware

Para que o laboratório 10 possa garantir a sua principal função (prestação de serviços) é importante que sejam garantidas condições para que o seu ***hardware*** esteja disponível de forma constante. No **contrato** com os **fornecedores** dos ativos é importante que a instituição garanta que o **fabricante ou o fornecedor certificado** faça uma **validação** e **verificação periódica** aos **ativos**.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 BAI03.05;

- ISO/IEC 27001:2013 A.11.2.4;
- NIST SP 800-53 Rev. 4 SA-10, SI-7.

PR.PI - Procedimentos e Processos de Proteção da Informação

PR.PI-1 - Deve ser criada e mantida uma configuração base de redes e sistemas de informação que incorpore os princípios de segurança

Deve ser definida uma **configuração base** para as redes e sistemas de informação do laboratório 10, tais como para os ativos e comunicações/conetividades.

Estas configurações base definem-se por:

- **programas informáticos** instalados nos computadores da sala de aula do laboratório 10;
- **servidores** e as **versões e atualizações** de sistemas operativos e aplicações, topologia da rede e estrutura lógica das arquiteturas das redes e sistemas de informação;
- Pela parte técnica, devem ser implementados "***sistemas de integração contínua (CI)***, ***sistemas de entrega contínua (CD)*** *e sistemas de gestão de atualizações de segurança*". (Centro Nacional de Cibersegurança, 2019)quad

Pela parte documental, devem ser **documentados, desenvolvidos e mantidos** todos os **controlos de versões** às configurações atuais das redes e sistemas de informação e, por fim, deve ser **criada, documentada e armazenada** uma **política de segurança das redes e sistemas de informação** do laboratório 10. Esta política terá de contemplar a aplicação dos **princípios mínimos de funcionalidades necessárias** e a **autorização ou proibição** da utilização de algumas funções, protocolos e serviços.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 3, 9, 11;
- COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05;
- ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4;
- NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10.

PR.PI-2 - Deve ser implementado um ciclo de vida de desenvolvimento seguro de software

A instituição deve aplicar "*princípios de* ***engenharia de segurança da informação*** *na* ***especificação***, ***desenho***, ***desenvolvimento***, ***implementação*** *e* ***modificação*** *das* ***redes e sistemas de informação***" **do laboratório 10**. Estes princípios devem ser aplicados em novos sistemas ou sistemas que sofram alterações significativas, sendo que em sistemas mais antigos é necessário ter em conta o *hardware*, *software* e o *firmware* atualmente implementado. (Centro Nacional de Cibersegurança, 2019)

A implementação técnica destes princípios pode passar pela implementação/utilização de uma **ferramenta de integração contínua** (CI), utilização de uma **ferramenta de controlo de versões** para gestão do código e, por fim, uma **ferramenta de gestão documental**, onde deverá estar armazenada toda a documentação sobre as redes e sistemas de informação.

A instituição deverá definir quais os **requisitos de segurança da informação**. Relativamente ao ciclo de vida de desenvolvimento de redes e sistemas de informação, devem ser implementadas proteções multicamadas, definidos princípios de segurança mínimos, definidas as fronteiras físicas e lógicas e as áreas de ataque e, não menos importante, a "*identificação de casos de uso, ameaças, perfis de atacantes, vetores e padrões de ataque*". (Centro Nacional de Cibersegurança, 2019)

As funções e responsabilidades no ciclo de vida de desenvolvimento devem ser definidas e documentadas, tal como os colaboradores que têm preocupação com a segurança

da informação no mesmo ciclo, com base nas suas funções. A gestão do risco de segurança da informação deve ser integrada no ciclo de vida de desenvolvimento.

A nível de documentação, deverão ser apresentados documentos onde estão definidos os "*requisitos de segurança da informação, a política de desenvolvimento seguro de software e o registo da execução de testes de segurança de software*". (Centro Nacional de Cibersegurança, 2019)

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 18;
- COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03;
- ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5;
- NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17.

PR.PI-3 - Deve ser implementado um processo de gestão de alterações

O processo de gestão de alterações passa pela implementação de diferentes sistemas, tais como: "*sistema de gestão de alterações, sistemas de integração (CI) e entrega (CD) contínua e um sistema de controlo de versões para configurações e código fonte*". (Centro Nacional de Cibersegurança, 2019)

A **configuração base das redes e sistemas de informação** deve ser formalmente **revista**, com base nos conceitos de funcionalidade mínima e políticas de fortalecimento de segurança previamente definidas.

Os **procedimentos de gestão de alterações**, após a sua criação, deverão ser documentados com a seguinte informação: as **alterações às redes e sistemas de informação** necessários, os **ativos** que podem sofrer com essas alterações, seja direta ou indiretamente, o **processo de aprovação ou reprovação das alterações**, os **métodos de execução**, os **testes**

às alterações, e os **métodos de recuperação** (se aplicável) e, por fim, as decisões tomadas e as alterações efetuadas.

Antes da implementação das alterações as mesmas deverão ser analisadas para detetar os possíveis impactos de segurança.

O processo de gestão de alterações deverá estar documentado, tal como os registos da execução do mesmo.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 3, 11;
- COBIT 5 BAI01.06, BAI06.01;
- ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4;
- NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10.

PR.PI-4 - Devem ser realizadas, mantidas e testadas cópias de segurança dos dados da organização

É importante que as **cópias de segurança** estejam sempre **atualizadas** para que possam ser utilizadas sempre que é necessário executar um restauro das mesmas.

As cópias de segurança devem ser **testadas e registadas** com regularidade e em períodos definidos e **validadas** de forma a comprovar a sua **integridade, confidencialidade e disponibilidade**. Cópias de segurança essas que devem ser realizadas com regularidade relativamente aos **dados dos utilizadores e das redes e sistemas de informação**. Em caso de falha devem ser tomadas medidas de correção das mesmas.

Por fim, nunca deve ser posta de parte a ideia de que estas cópias de segurança possam ser guardadas num local fora das instalações do laboratório 10/Maiêutica.

Toda a aplicabilidade destas medidas deve ser documentada e descrita como políticas de cópias de segurança e devem ser feitos registos tanto das cópias de segurança e dos seus restauros, como dos exercícios e testes feitos às mesmas.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 10;
- COBIT 5 APO13.01, DSS01.01, DSS04.07;
- ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3;
- NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9.

PR.PI-5 - As políticas e regulamentações associadas à operacionalização dos ambientes físicos dos ativos da organização devem ser seguidas

Atualmente, é essencial para o laboratório 10 a possibilidade de **acompanhar a operacionalidade do laboratório** como um todo. Esse acompanhamento passa pelo seguimento de políticas/regulamentações "*relativas à **proteção das redes e sistemas de informação contra desastres naturais**, **falhas de energia**, **incêndios** e **inundações***" (Centro Nacional de Cibersegurança, 2019).

Com o objetivo de acompanhar e proteger o máximo possível os ativos físicos do laboratório 10 devem ser implementadas algumas medidas, tais como: implementação de "***proteção contra picos de corrente elétrica**, **simplificar e tornar mais seguro o controlo de energia***" através da implementação de dispositivos físicos de sensores e atuadores, **adicionar um ou mais geradores de emergência ou UPS**, implementar **sensores de temperatura, humidade, fumo e inundação** pelo menos na sala técnica, **proteger a cablagem física** de acesso não autorizado, permitir que possam ser **desligadas as redes e sistemas de informação do laboratório 10 em caso de emergência**, proteger estes sistemas de que os possam ativar sem autorização e, por fim, **executar manutenção** aos mesmos, em períodos devidamente predefinidos. (Centro Nacional de Cibersegurança, 2019)

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 DSS01.04, DSS05.05;

- ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3;
- NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18.

PR.PI-6 - Os dados devem ser destruídos de acordo com a política definida

Os **dados**, que podem ser em formato **digital** ou **físico**, quando terminado o seu ciclo de vida, devem ser **destruídos** com base numa **política** definida para o efeito. Esta ação é importante para a segurança do laboratório 10, no sentido em que essas mesmas informações, utilizadas incorretamente, podem pôr em causa a segurança do mesmo. As informações devem ser destruídas com base na sua **classificação** (previamente documentada) e nas **leis** nacionais/setoriais previamente impostas.

A nível digital deve ser implementado um **sistema destruição de ficheiros** e a nível físico, um **destruidor de papel**. Quando a informação deixa de ser relevante (término do seu **ciclo de vida**), a Maiêutica e o laboratório 10 devem garantir que são controladas as destruições feitas à mesma. Quando a destruição for feita por terceiros, devem ser implementados controlos adicionais de forma a garantir que a destruição da informação foi feita corretamente. Por fim, terá de ser garantido o **registo da eliminação dos ativos**.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 BAI09.03, DSS05.06;
- ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7;
- NIST SP 800-53 Rev. 4 MP-6.

PR.PI-7 - Os processos de proteção devem ser continuamente melhorados

Os processos de **proteção** devem ser regularmente **avaliados e atualizados** de forma a serem detetas possíveis fragilidades e as mesmas possam ser corrigidas. Todos os

controlos, processos e sistemas de gestão devem ser periodicamente **monitorizados**, **analisados** e **auditados** internamente. As auditorias devem resultar em relatórios com a descrição dessas auditorias e em **planos de ação** para a aplicação das melhorias necessárias.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 APO11.06, APO12.06, DSS04.05;
- ISO/IEC 27001:2013 A.16.1.6, Cláusula 9, Cláusula 10;
- NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6.

PR.PI-8 - A efetividade das tecnologias de proteção deve ser tida em conta na melhoria dos processos de proteção

Com o objetivo de reduzir os riscos de ocorrências futuras, devem ser feitas **sessões** onde se **analisam os incidentes ocorridos** e quais as **conclusões** da análise desses incidentes, permitindo identificar quais as melhorias necessárias, levando, também, à modificação dos processos de proteção.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 BAI08.04, DSS03.04;
- ISO/IEC 27001:2013 A.16.1.6;
- NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4.

PR.PI-9 - Os planos de resposta a incidentes, continuidade de negócio, a recuperação de incidentes e recuperação de desastres devem ser atualizados

No caso do laboratório 10, os **planos de resposta e recuperação de incidentes**, a **recuperação de desastres** e a **continuidade da prestação de serviços** devem ser atualizados com frequência.

O plano de resposta e recuperação de incidentes deve conter um **plano de implementação da capacidade de resposta**, a **estrutura da primeira resposta**, a **definição de incidentes**, quais os **recursos necessários** para suportar esta resposta e qual a **resposta no caso de perda de informação**.

O **plano de continuidade da prestação de serviços** deve conter o **propósito**, o **âmbito**, os **papéis**, as **responsabilidades** e o **comprometimento da gestão de topo** e **coordenação com partes interessadas** externas. As **funções essenciais** ao bom funcionamento do laboratório 10 devem ser **identificadas**, tal como os **requisitos de contingência** das mesmas. As prioridades de **recuperação**, os **objetivos** e as **métricas** devem ser definidas de forma a se poder chegar ao objetivo final deste plano: a **recuperação total das funções essenciais** do laboratório 10.

Por fim, os planos de resposta e recuperação devem ser partilhados com as partes externas de maior importância e o plano de continuidade da prestação de serviços devem ser revistos com a maior regularidade possível.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 19;
- COBIT 5 APO12.06, DSS04.03;
- ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3;
- NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17.

PR.PI-10 - Os planos de resposta e recuperação devem ser testados e exercitados

Os **planos de resposta e de recuperação de incidentes** devem ser testados de forma a **validar a sua eficácia** e, no caso de haver falhas, que possam ser corrigidas. É aconselhável que sejam feitos **simulacros de casos reais** e que sejam registados a **execução e resultados** (testes de reposta/recuperação de incidentes).

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 19, 20;
- COBIT 5 DSS04.04;
- ISO/IEC 27001:2013 A.17.1.3;
- NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14.

PR.PI-11 - A cibersegurança deve ser contemplada nos processos de gestão de recursos humanos

A triagem na contratação de recursos humanos também é importante para o processo de melhoria de segurança do laboratório 10. Desde a **triagem** dos candidatos, a **contratação**, a **categorização** de posições e até mesmo a **vinculação** laboral devem ser definidos processos com base em requisitos de segurança previamente estabelecidos.

É importante a Maiêutica definida **processos de gestão dos recursos humanos** (entrada, modificação e saída). Esses processos devem ter cuidados como a categorização da posição (funções, âmbito, responsabilidades e risco).

No caso de **transferência** do colaborador, devem ser revistos os diversos tipos de acessos possivelmente atribuídos a esse colaborador ao laboratório 10 e a todas as redes e sistemas de informação e atualizar os mesmos conforme nas novas funções. No caso de **cessação** total com a instituição, é necessário cancelar todos os acessos físicos e lógicos relativos àquele colaborador.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 5, 16;
- COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05;
- ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4;
- NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21.

PR.PI-12 - Deve ser definido e implementado um processo de gestão de vulnerabilidades

É importante, também, a criação de um **processo de gestão das vulnerabilidades**. Esse processo tem de ser constituído pelos seguintes requisitos:

- Deve ser feito um planeamento que permita **rastrear as vulnerabilidades**, de forma a contemplar a sequência da execução desse rastreio, as janelas temporais da sua execução e um relatório final com todas as vulnerabilidades detetadas;
- Devem ser analisados todos os relatórios relativos às vulnerabilidades e definidas as **respostas** a serem executadas;
- As decisões do **tratamento de vulnerabilidades** devem estar proporcionais com a tolerância ao risco do laboratório 10, anteriormente definida (gestão do risco);
- A informação sobre as vulnerabilidades deve ser **partilhada pela equipa técnica** da Maiêutica e do laboratório 10, para que estes possam estar sempre atentos a possíveis situações similares;
- Conforme o tipo de vulnerabilidade, a informação sobre a mesma deve ser partilhada com as entidades externas.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 4, 18, 20;
- COBIT 5 BAI03.10, DSS05.01, DSS05.02;

- ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3;
- NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2.

PR.MA- Manutenção

PR.MA-1 - As atividades de manutenção e reparação dos ativos da organização devem ser realizadas e registadas em programas e planos aprovados e controlados

A **manutenção dos ativos** do laboratório 10 deve ser feita com **regularidade**, sendo que "*deve ser registada, efetuada e supervisionada por colaboradores*" previamente definidos para essa função com base nas suas competências (lista de pessoas autorizadas).

O processo de manutenção de sistemas deve ser **desenvolvido**, **implementado**, **revisto** e **atualizado** e deve estar descrito o "***âmbito***, *o* ***propósito***, *os* ***perfis*** *e as* ***responsabilidades*** *das partes envolvidas*". Os registos de manutenção devem ser planeados, executados e documentados, sendo necessário **pré-definir janelas temporais** para a manutenção a ativos críticos presentes no laboratório 10. (Centro Nacional de Cibersegurança, 2019)

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05;
- ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6;
- NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6.

PR.MA-2 - As operações de manutenção remota das redes devem ser revistas, aprovadas, executadas e registadas

A **manutenção remota** das redes e sistemas de informação do laboratório 10 deve ser **aprovada** e **monitorizada**. Esta aprovação e monitorização permitirá, respetivamente, o **impedimento de acessos não autorizados** e o **registo** desses mesmos acessos.

Devem ser utilizados **mecanismos de autenticação fortes** nas ligações e garantir que, no final da manutenção, todas as **ligações** são **terminadas**.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 3, 5;
- COBIT 5 DSS05.04;
- ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1;
- NIST SP 800-53 Rev. 4 MA-4.

PR.TP- Tecnologia de Proteção

PR.TP-1 - Os registos de auditoria e de histórico devem ser documentados, implementados e revistos de acordo com as políticas

Os registos de auditorias e de histórico devem ser **definidos**, "***documentados***, ***implementados*** *e* ***revistos***". De forma a uniformizar os registos, a **política de gestão de eventos, registos de auditoria e histórico** deve ser **criada**, **divulgada**, **revista** e **atualizada**, tal como os procedimentos de recolha dos registos e dos eventos. Na mesma política deve ser descrita a justificação pela qual este tipo de registos é importante para a análise de incidentes. (Centro Nacional de Cibersegurança, 2019)

Devem ser definidos os **tipos de registos de auditoria** que podem ser aplicados nas redes e sistemas de informação do laboratório 10. Os eventos necessários de registos de

auditoria devem ser identificados. A taxonomia dos registos de auditoria permite a definição dos parâmetros que deverão fazer parte desses mesmo registos, "*por exemplo:* ***quando***, ***onde***, ***o quê***, ***quem*** *e* ***porquê***". (Centro Nacional de Cibersegurança, 2019)

É necessário garantir que o local onde vão ser guardados estes registos tenha **capacidade de armazenamento suficiente** para os mesmos e quais os **períodos de retenção** da informação. Os registos devem estar devidamente sincronizados (fonte e fuso horário).

Por fim, deve ser verificado se as redes e sistemas de informação têm capacidade para proteger os registos de auditoria (acessos indevidos, modificação ou remoção) e não os recusar.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 1, 3, 5, 6, 14, 15, 16;
- COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01;
- ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1;
- NIST SP 800-53 Rev. 4 família AU.

PR.TP-2 - Os suportes de dados amovíveis devem ser protegidos e a sua utilização deve ser restrita, de acordo com a política definida

A **informação** deve ser **classificada** e devidamente **documentada** para que se possa cumprir as regras de utilização de suporte de dados amovíveis.

A criação de uma **política de cifra de informação** vai permitir fazer uma **gestão de cifras** no caso da **transferência de dados** para dispositivos amovíveis. O **acesso físico** deve ser devidamente **restringido**, no caso, por exemplo, dos armários presentes no laboratório 10 e é importante, também, **não possibilitar** a inserção de **dispositivos amovíveis**. No **acesso** à parte **lógica** devem ser executados mecanismos que **não permitam a alteração de dados**, por exemplo, por *software*. As restrições acima mencionadas devem ser feitas com base na **classificação** anteriormente definida.

Por fim, devem ser disponibilizados **programas de destruição e higienização** de ficheiros, sempre tendo em conta a classificação da informação.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 8, 13;
- COBIT 5 APO13.01, DSS05.02, DSS05.06;
- ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9;
- NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8.

PR.TP-3 - O princípio da minimização de funcionalidades deve ser incorporado na configuração de sistemas de modo a fornecer apenas os recursos essenciais

A aplicação do **princípio de funcionalidade mínima** vai garantir que os utilizadores apenas têm acesso ao que necessitam para cumprir as suas funções. Com este princípio devem ser implementadas diversas restrições, tais como: de **portos**, **protocolos** e **serviços**, de **processos**, de **níveis de privilégios mínimos**, de **acesso** a funções de **segurança** e a **comandos privilegiados** da rede, de **contas privilegiadas** e de privilégios para a **execução de código**.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 3, 11, 14;
- COBIT 5 DSS05.02, DSS05.05, DSS06.06;
- ISO/IEC 27001:2013 A.9.1.2;
- NIST SP 800-53 Rev. 4 AC-3, CM-7.

PR.TP-4 - As redes de comunicações e de controlo devem ser protegidas

"*Os fluxos regulam a transferência de informação e os caminhos que podem ser abertos dentro de cada sistema ou entre sistemas.*" (Centro Nacional de Cibersegurança, 2019)

A implementação técnica passa pela adoção do uso das seguintes componentes tecnológicas: "***Sistema de Deteção e Prevenção de Intrusões (IDS/IPS)***, ***Firewall***, ***Proxy*** *e* ***Firewall de aplicações web (WAF)***". (Centro Nacional de Cibersegurança, 2019)

Todas as alterações que sejam necessárias ser feitas tanto a nível dos fluxos de dados, como das redes de comunicação devem ser sujeitas a uma requisição prévia.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 8, 12, 15;
- COBIT 5 DSS05.02, APO13.01;
- ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3;
- NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43.

PR.TP-5 - Devem ser implementados mecanismos para cumprir os requisitos da resiliência em situações adversas

No laboratório 10 é bastante importante a existência de **redundância** dos sistemas. É necessário que sejam implementados mecanismos que permitam cumprir requisitos de **resiliência** mínimos em situações anormais e garantir que são alocados recursos/equipamentos extras.

A definição do tempo máximo aceitável de falha para ativos/recursos críticos é importante para serem fornecidos componentes de substituição no caso de avaria dos componentes atuais. Deverá ser garantida a disponibilidade das redes e sistemas de informação, quando são detetadas as condições previamente definidas.

A disponibilidade das redes e dos sistemas de informação deve ser garantida alocando os recursos necessários e prioritizar os sistemas com base na sua criticidade.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05;
- ISO/IEC 27001:2013 A.17.1.2, A.17.2.1;
- NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6.

Detetar

A medida de segurança Detetar tem como objetivo a organização compreender o seu enquadramento, os ativos que auxiliam os processos críticos da mesma e os riscos diretamente associados. A compreensão destes pontos "*permite que a organização consiga definir e priorizar os seus recursos e investimentos de acordo com os seus objetivos gerais e com a sua estratégia de gestão do risco.*" (Centro Nacional de Cibersegurança, 2019)

Esta medida de segurança é constituída por três categorias (**DE.AE**, **DE.MC** e **DE.PD**) e de subcategorias um mínimo de cinco e um máximo de oito.

DE.AE – Anomalias e Eventos

DE.AE-1 – A organização deve definir e gerir um modelo de referência de operações de rede e fluxos de dados esperados para utilizadores e sistemas

As a**lterações feitas na infraestrutura** de rede de comunicações do laboratório 10 devem ser executadas de forma **regulada**, por colaboradores devidamente qualificados e que esteja garantida a **integridade**, **confidencialidade** e **disponibilidade** da informação.

Relativamente ao **fluxo de comunicações**, devem ser estudados e analisados **padrões de referência,** previamente criados, independentemente da origem dos mesmos (utilizadores ou sistemas internos). Os padrões devem ser atualizados com base em possíveis alterações nas redes e sistemas de informação, sendo que essas alterações devem ser feitas seguindo o processo de gestão de alterações.

A implementação técnica passa pela adoção do uso das seguintes componentes tecnológicas: "***Sistema de Deteção e Prevenção de Intrusões (IDS/IPS)***, ***Firewall***, ***Proxy*** *e* ***Firewall de aplicações web (WAF)***". (Centro Nacional de Cibersegurança, 2019)

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 1, 4, 6, 12, 13, 15, 16;

- COBIT 5 DSS03.01;
- ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2;
- NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4.

DE.AE-2 – Os eventos detetados devem ser analisados por forma a se identificarem os alvos e os métodos de ataque

As redes e sistemas de informação do laboratório 10 devem ser **monitorizados** de forma a ser **analisados os possíveis eventos** que possam ter ocorrido. Devem estar previamente definidos mecanismos processuais que permitam **gerir os eventos** e definir quais devem ser avaliados com maior detalhe. Estes mecanismos devem garantir que, sobre cada evento, é recolhida o máximo de informação possível para que se possa identificar a **origem**, **alvos** e os **métodos** de **ataque** utilizados. Se se confirmar que existiu um incidente, o mesmo deve ser identificado.

Todos os passos explicados anteriormente fazem parte de um processo de gestão e de correlação de eventos de segurança, que deve ser devidamente documento, tal como a gestão de incidentes e a resposta aos mesmos.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 3, 6, 13, 15;
- COBIT 5 DSS05.07;
- ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4;
- NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4.

DE.AE-3 – Os eventos devem ser coletados e correlacionados a partir de várias fontes e sensores

Nas redes e sistemas de informação do laboratório 10 deverão ser implementados **mecanismos tecnológicos e processuais** para a **recolha e correlação de eventos** gerados nos mesmos e em outros dispositivos de segurança. Esta correlação deverá ser valorizada com o acréscimo de todo o **conhecimento** encontrado em **fontes externas** sobre ameaças.

Os ***honeypots*** são o mecanismo aconselhado como sensor de alertas na rede de comunicações. No contexto do laboratório 10, os ***logs*** em **equipamentos de *core*** também deverão ser armazenados e analisados, sendo necessário o auxílio de uma plataforma que envie **alertas** quando detetar que a informação armazenada não vai de encontro ao que está estipulado.

A recolha dos **eventos** de segurança nos **sistemas de informação**, dos **equipamentos de rede** de comunicação e dos **dispositivos de segurança** deverão ser armazenados, o que permitirá efetuar uma **correlação dos eventos entre si**, com **incidentes passados** e com **fontes de conhecimento externas**.

Por fim, deverá ser ponderada a **relevância da partilha** de incidentes de segurança, independentemente do estado atual do incidente, com **autoridades**, **terceiros**, **alunos** e **docentes**, conforme for aplicável.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16;
- COBIT 5 BAI08.02;
- ISO/IEC 27001:2013 A.12.4.1, A.16.1.7;
- NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4.

DE.AE-4 – O impacto dos eventos deve ser classificado

Os eventos devem ser **categorizados** e **tipificados**, permitindo que possa ser medido o **impacto** deles nas redes e sistemas de informação do laboratório 10. A atribuição destas características vai permitir a ação sobre um determinado evento, pois estes podem se tornar facilmente em incidentes (ativação do processo de gestão de incidentes).

Este processo deverá gerar um documento de suporte à gestão de eventos, registos da tipificação dos eventos e uma análise à ligação entre a gestão de eventos e a gestão de incidentes.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 4, 6;
- COBIT 5 APO12.06, DSS03.01;
- ISO/IEC 27001:2013 A.16.1.4;
- NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4.

DE.AE-5 – Devem ser definidos os limites de alerta para incidentes

A **abertura de incidentes** deve ser justificada e feita com base na **categorização** e **tipificação** de **eventos** no sistema de gestão de eventos.

Deve ser **classificada** a **prioridade** de cada incidente, definindo quais os **limites** de um evento, **conjunto de eventos** ou a correlação dos mesmos, para a abertura de um incidente. Essa prioridade pode aumentar ou diminuir com base nos limites previamente definidos para um incidente de cibersegurança.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 6, 19;

- COBIT 5 APO12.06, DSS03.01;
- ISO/IEC 27001:2013 A.16.1.4;
- NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8.

DE.MC – Monitorização Contínua de Segurança

DE.MC-1 – As redes e sistemas de informação devem ser monitorizados para detetar potenciais incidentes

Durante o **processo de gestão de eventos**, deve ser feita a monitorização das redes e sistemas de informação do laboratório 10. A **monitorização** deve ser **contínua** e apoiada pelo uso de ***software* de gestão de eventos**, **sistemas de detenção** e **prevenção de intrusões** (acessos não autorizados) e ***firewall***.

A gestão e correlação de eventos e a gestão de incidentes deve ser devidamente documentada.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 1, 7, 8, 12, 13, 15, 16;
- COBIT 5 DSS01.03, DSS03.05, DSS05.07;
- NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4.

DE.MC-2 – O ambiente físico deve ser monitorizado para se detetar potenciais incidentes de segurança

É extremamente importante que possam ser garantidas condições que permitam a **monitorização do perímetro físico** do laboratório 10. Inseridos no processo de gestão de eventos, os **controlos de proteção física** podem ser aplicados com o uso de **soluções de**

CCTV, tendo em atenção o RGPD (Comissão Europeia, 2016b), **controlos de acesso** e **gestão de eventos de segurança da informação** (tipificação e categorização específica).

Os resultados do controlo de segurança física devem criar registos de auditoria. Esses registos devem ser armazenados e relacionados com o sistema de gestão de eventos de segurança da informação. Por fim, devem ser criados alertas que sejam ativos após a deteção de acessos não autorizados.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 DSS01.04, DSS01.05;
- ISO/IEC 27001:2013 A.11.1.1, A.11.1.2;
- NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20.

DE.MC-3 – A atividade dos colaboradores deve ser monitorizada para se detetar potenciais incidentes

A **monitorização dos colaboradores** do laboratório 10 é importante para o processo de gestão de eventos, sempre respeitando o "*enquadramento jurídico aplicável e a política de privacidade*" do laboratório 10. Esta monitorização vai permitir que se possam tomar medidas mais rapidamente no caso de ser detetado algum incidente proveniente da atividade desse colaborador. (Centro Nacional de Cibersegurança, 2019)

A monitorização vai permitir fazer uma **correlação das atividades dos colaboradores** com padrões de utilização ditos normais e deve estar também presente sempre que for necessário um acesso privilegiado às redes e sistemas de informação do laboratório 10. Deverão estar programados **alertas** que, quando necessário, poderão fazer com que um evento possa passar a ser considerado um incidente. Estes alertas deverão também ser documentados com o **tipo de evento** e o qual o **comportamento anómalo** por parte do colaborador.

De ter atenção que devem ser sempre garantidos os princípios de proteção e tratamentos de dados dos utilizadores.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 5, 7, 14, 16;
- COBIT 5 DSS05.07;
- ISO/IEC 27001:2013 A.12.4.1, A.12.4.3;
- NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11.

DE.MC-4 – A organização deve identificar e implementar mecanismos para deteção de código malicioso

A Maiêutica tem de garantir a criação de **mecanismos** que tenham o objetivo de **detetar** e **proteger** as **redes** e **sistemas de informação** do laboratório 10 da existência de código malicioso. Os mecanismos devem produzir **registos de auditoria**, sendo que esses registos devem ser **recolhidos** e **relacionados** no **sistema de gestão de eventos**.

Ferramentas devem ser implementadas de forma a **detetar/proteger contra código malicioso** os **equipamentos** disponíveis no laboratório 10 para as aulas/testes práticos. Estas ferramentas deverão fazer **verificações periódicas** e em **tempo real** nas redes e sistemas de informação, análises aos ficheiros provenientes de **origens externas** (ficheiros com origem da *internet*, de suportes amovíveis, entre outros). No caso de ser **detetado** um código malicioso, as ferramentas deverão ter a capacidade de **responder** de imediato, bloqueando e colocando o mesmo em quarentena. Para além disso, é necessário analisar possíveis dependências de bibliotecas externas. Por fim, devem ser geridos e correlacionados todos os eventos de segurança da informação.

A **instituição** tem de garantir a criação de **alarmística** específica que vai auxiliar a deteção e prevenção de código malicioso, a orientação de **falsos positivos** e qual o potencial

do impacto deste mesmo código nos sistemas do laboratório 10 e, por fim, garantir uma análise constante da técnica do código fonte desenvolvido.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 4, 7, 8, 12;
- COBIT 5 DSS05.01;
- ISO/IEC 27001:2013 A.12.2.1;
- NIST SP 800-53 Rev. 4 SI-3, SI-8.

DE.MC-6 – As atividades dos prestadores de serviços externos devem ser monitorizadas para deteção de incidentes

Na **política de gestão dos fornecedores**, para além dos **requisitos de segurança**, os **perfis** e as **responsabilidades** para os fornecedores, devem estar identificadas as **atividades de monitorização dos serviços** externos de forma a detetar o **acesso indevido** às redes e sistemas de informação do laboratório 10. No caso de **colaboradores gerarem eventos**, devem ser investigados todos os **possíveis incidentes** que possam derivar desse evento.

Por fim, a Maiêutica deve garantir que os **prestadores de serviços** sigam as **políticas de segurança** previamente estabelecidas, que os **colaboradores** respeitem a **confidencialidade da informação** e que no caso de algum colaborador não trabalhar mais com a organização, deverá ser reportada essa situação à Maiêutica.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 APO07.06, APO10.05;
- ISO/IEC 27001:2013 A.14.2.7, A.15.2.1;
- NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4.

DE.MC-7 – Deve ser efetuada a monitorização de acessos não autorizados de colaboradores, conexões, dispositivos e software

A instituição deverá monitorizar os **acessos às redes e sistemas de informação** do laboratório 10 por "***colaboradores***, ***dispositivos***, ***equipamentos*** *e* ***processos***" que não tenham autorização. Devido ao contexto e funcionamento do laboratório 10, nem sempre a monitorização de acesso será aplicável pois, ou se faz um levantamento no início de cada ano letivo e exclusão no fim do mesmo, ou então serão gerados alertas sempre que, por exemplo, os alunos ligarem os seus equipamentos à rede do laboratório 10. (Centro Nacional de Cibersegurança, 2019)

Independentemente da implementação feita, é boa prática a **recolha de dados** para uma localização específica, de forma a facilitar a análise desses dados pelo *software* de monitorização, permitindo a deteção mais eficaz de acessos indevidos. Se esses acessos forem **detetados**, os **eventos** por eles gerados deverão ser **reportados**. Como qualquer evento, os mesmo podem se tornar incidentes, sendo necessário investigar e proceder à sua resolução.

A nível documental, deverão ser feitos registos de todos os eventos de acessos a sistemas de informação, registos de correlação de acessos não autorizados a eventos e, por fim, relatórios de incidentes que derivem desses mesmo eventos.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16;
- COBIT 5 DSS05.02, DSS05.05;
- ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1;
- NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4.

DE.MC-8 – Devem ser efetuados rastreios de vulnerabilidades

O **processo de gestão de vulnerabilidades** anteriormente definido deve ser aplicado de forma a serem feitos **rastreios regulares**, automáticos ou manuais.

Estes rastreios devem estar **previstos** num **plano de execução das análises** de vulnerabilidades. Quando são encontradas **falhas**, devem ser documentadas quais as **plataformas**, **versões**, **falhas** e **configurações incorretas**, o **impacto** e **descrição** das vulnerabilidades, quais os **procedimentos de correção** e um **teste de validação** de falsos positivos.

Quando aplicável, devem ser feitas correções/mitigações, devidamente documentadas, tal como o processo de gestão de vulnerabilidades e a análise de vulnerabilidades.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 5, 7, 14, 16;
- COBIT 5 DSS05.07;
- ISO/IEC 27001:2013 A.12.4.1, A.12.4.3;
- NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11.

DE.PD – Processos de Deteção

DE.PD-1 – Devem ser definidos os papéis e responsabilidades na deteção de eventos anómalos

Nos **processos de gestão de eventos e de incidentes**, anteriormente documentados, devem ser definidas as **partes interessadas**, as **funções** e **responsabilidades** das mesmas e

em que **momento do processo** as mesmas intervêm. Também devem ser definidos os **processos de escalonamento** e qual a **taxonomia de classificação de eventos**.

Após todo este processo, devem ser dadas **sessões de esclarecimento** de forma a indicar às partes interessadas quais os limites de responsabilidade e as respetivas atividades.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 19;
- COBIT 5 APO01.02, DSS05.01, DSS06.03;
- ISO/IEC 27001:2013 A.6.1.1, A.7.2.2;
- NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14.

DE.PD-2 – As atividades de deteção devem cumprir com todos os requisitos aplicáveis

As **auditorias internas** devem ser implementadas de forma a verificar a **funcionalidade dos serviços de deteção** e a identificar **possíveis melhorias**.

Deverá ser feito um plano de auditorias internas **anuais**, devidamente documentado, onde está descrito a **metodologia de avaliação**, se os "***ambientes***, ***papéis***, ***responsabilidades*** *e* ***equipas*** *estão definidos*" e verificar se as **atividades de detenção** estão em conformidade e em funcionamento de forma adequada ao que é pretendido. (Centro Nacional de Cibersegurança, 2019)

No caso de serem detetadas oportunidades de melhoria, deve ser feito um plano de atividades e registar quais as ações de melhoria aplicadas.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 DSS06.01, MEA03.03, MEA03.04;
- ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3;

- NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14.

DE.PD-3 – Os processos de deteção devem ser testados

A verificação do **funcionamento** e os **testes** feitos aos **sistemas de deteção** devem ser executados sempre que existir alguma **alteração significativa nos sistemas**, quando existo um **novo desenvolvimento aplicacional** igualmente significativo, quando é executado um **novo sistema na infraestrutura** do laboratório 10 e quando for **detetada uma vulnerabilidade**.

O **plano de testes** deve passar pela identificação dos **objetivos** do mesmo e a elaboração de um **relatório com as atividades a executar**. Após a execução dos testes, será necessário avaliar os **resultados obtidos** de forma a detetar a necessidade de aplicar melhorias, se for esse o caso, terá de ser elaborado um plano de implementação de melhorias.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 APO13.02, DSS05.02;
- ISO/IEC 27001:2013 A.14.2.8;
- NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14.

DE.PD-4 – Informações sobre deteções de eventos devem ser comunicadas

O **plano de comunicação de ocorrência de eventos e/ou incidentes** tem como objetivo manter as **partes interessadas informadas** sobre os mesmos. O plano de comunicação, que parte do **processo de gestão de incidentes**, deve ser constituído pelas seguintes informações:

"*1) O que comunicar: Que conteúdo (por exemplo: a descrição de um incidente e os seus impactos);*

2) Que mensagem: Forma e formato, que tipo de meio será usado, desde pequenos textos a imagens, metáforas, vídeos, entre outros;

3) Quem deve comunicar: Deve ser nomeado um responsável que tenha a autoridade e autonomia para comunicar, particularmente com organizações externas;

4) A quem comunicar: Destinatários da comunicação;

5) Como comunicar: Que canais devem ser usados para obter maior eficácia na difusão da mensagem (por exemplo: mensagens de correio eletrónico, protetores de ecrã);

6) Quando comunicar: A comunicação deve ser regularmente exercitada em condições comuns (por exemplo: divulgação da política de segurança da informação), mas poderá ter frequências e modos de atuação muito diferentes em contexto de incidente." (Centro Nacional de Cibersegurança, 2019)

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 19;
- COBIT 5 APO08.04, APO12.06, DSS02.05;
- ISO/IEC 27001:2013 A.16.1.2, A.16.1.3;
- NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4.

DE.PD-5 – Os processos de deteção devem ser objeto de melhoria continua

A execução de um "***procedimento de revisão e aprendizagem*** *de processos de deteção de eventos*" vai garantir que se teve **conhecimento dos incidentes** previamente ocorridos nas redes e sistemas de informação do laboratório 10. Com esta aprendizagem são possíveis a criação de um "***plano de melhoria dos processos de detenção*** *e o* ***registo de tratamento*** *de ações de melhoria*" identificadas no plano de testes aos processos de detenção. (Centro Nacional de Cibersegurança, 2019)

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 APO11.06, APO12.06, DSS04.05;
- ISO/IEC 27001:2013 A.16.1.6;
- NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14.

Responder

O objetivo da medida de segurança Responder é definir e implementar medidas no caso de deteção de incidentes. As medidas propostas ao longo desta medida permitem "*mitigar o impacto do incidente, ou seja, reduzir os seus potenciais efeitos adversos*". (Centro Nacional de Cibersegurança, 2019)

Esta medida de segurança é constituída por cinco categorias (**RS.PR**, **RS.CO**, **RS.AN**, **RS.MI** e **RS.ME**) e as subcategorias têm um mínimo de um e um máximo de cinco.

RS.PR – Planeamento da Resposta

RS.PR-1 - O plano de resposta deve ser executado durante ou após a ocorrência de um incidente

O **processo de resolução dos incidentes** deve ser **sistematizado**, onde será identificado o **responsável pelo tratamento** dos mesmos (coordenação de atividades de resposta e contingência) e que permita garantir a correta **alocação dos recursos humanos**, **tecnológicos** e **processuais** para uma resolução mais eficaz dos incidentes, incluindo as fases de contenção e de erradicação.

A **análise de evidências** dos incidentes deve garantir a **integridade das evidências** que foram recolhidas e analisadas. Para os incidentes deve ser criado um **processo de escalonamento dos mesmos**.

Como resultado das atividades de resposta aos incidentes, deve ser garantido que o rigor, âmbito, aplicabilidade e resultados das mesmas é transversal e consistente a todos os incidentes.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 19;
- COBIT 5 APO12.06, BAI01.10;

- ISO/IEC 27001:2013 A.16.1.5;
- NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8.

RS.CO – Comunicações

RS.CO-1 – Na resposta a um incidente, os colaboradores devem conhecer os seus papéis e a ordem de execução de atividades

Na **resposta** a um incidente é importante garantir que os colaboradores da Maiêutica/laboratório 10 têm **conhecimento das partes interessadas envolvidas**, do **papel no processo de resposta** e quais os **passos de resolução** do mesmo. Os colaboradores podem adquirir esse conhecimento através de **ações de sensibilização**, onde será apresentado o **processo de resposta a incidentes**. Esse processo contém informação como: quais são as **partes interessadas**, quais os **papéis** e as **responsabilidades** de cada interveniente e quais os **passos a serem executados como resposta** a esses mesmos incidentes.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 19;
- COBIT 5 EDM03.02, APO01.02, APO12.03;
- ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1;
- NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8.

RS.CO-2 – Os incidentes devem ser reportados de acordo com critérios estabelecidos

No **plano de resposta a incidentes** devem ser identificados quais os **canais de divulgação de incidentes** às partes interessadas e qual a **tipificação e classificação** de incidentes de segurança da informação definida. Caso seja necessário, também deverá ser

definido o "***processo de notificação e comunicação de incidentes*** *a* ***autoridades*** *ou a* ***terceiros*****"**. (Centro Nacional de Cibersegurança, 2019)

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 19;
- COBIT 5 DSS01.03;
- ISO/IEC 27001:2013 A.6.1.3, A.16.1.2;
- NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8.

RS.CO-3 – As informações devem ser partilhadas de acordo com o plano de resposta

As **informações de incidentes** terão de ser do conhecimento de todas as **partes interessadas**. Esse conhecimento poderá ajudar as mesmas a "***detetar***, ***conter*** *e* ***solucionar*** *problemas semelhantes nos seus sistemas de informação*". A instituição deverá reportar essa informação em **tempo útil** e através de **canais de comunicação seguros**. (Centro Nacional de Cibersegurança, 2019)

Todos os planos de comunicação podem ser consolidados com os planos de comunicação previamente definidos.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 19;
- COBIT 5 DSS03.04;
- ISO/IEC 27001:2013 A.16.1.2, Cláusula 7.4, Cláusula 16.1.2;
- NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4.

RS.CO-4 – A coordenação com as partes interessadas deve ocorrer conforme os planos de resposta

O **plano de comunicação**, **coordenação** e de **escalonamento** de incidentes deve ser implementado com base na categorização e criticidade dos incidentes.

Para a **implementação** do **plano de resposta a incidentes**, é importante **identificar**, como mencionado nas subcategorias anteriores, as seguintes informações: as **partes interessadas relevantes**, o **plano de comunicação** (que está descrito na subcategoria **DE.PD-4** e, de acrescentar, o **ponto único de contacto** com cada uma das partes interessadas), as **responsabilidades**, os **limites de atuação**, o **tempo de resposta** de cada uma das diferentes partes e os **contactos de autoridades**, no caso de ser necessário.

Toda esta implementação deve ser suportada por documentos do plano de resposta a incidentes e por relatórios de resposta a incidentes anteriores.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 19;
- COBIT 5 DSS03.04;
- ISO/IEC 27001:2013 Cláusula 7.4;
- NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8.

RS.CO-5 – Deve ocorrer partilha voluntária de informação com partes interessadas externas

No **processo de resposta aos incidentes** deve estar contemplada a **possibilidade de a informação** ser partilhada com as partes interessadas externas e qual a **informação** que é necessária partilhar. O objetivo desta partilha é que sejam **identificados os indicadores de compromisso** e que as partes interessadas possam, também, **melhorar o tempo de**

identificação, **deteção**, **contenção** e **erradicação** dessas ameaças no seu círculo de influência.

Como foi mencionado ao longo de toda a categoria **RS.CO**, é importante manter uma **lista atualizada das partes interessadas** e também **canais seguros** para garantir uma partilha de informação sempre segura com as partes externas interessadas.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 19;
- COBIT 5 BAI08.04;
- ISO/IEC 27001:2013 A.6.1.4;
- NIST SP 800-53 Rev. 4 SI-5, PM-15.

RS.AN – Análise

RS.AN-1 – As notificações dos sistemas de deteção devem ser investigadas

A Maiêutica deve garantir que os **eventos** que podem evoluir para **incidentes** sejam devidamente detetados e identificados. Posto isso, esses eventos, com origem nos sistemas de deteção, devem ser "***analisados***, ***categorizados*** *e* ***tratados*** *de forma sistematizada*". (Centro Nacional de Cibersegurança, 2019)

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 4, 6, 8, 19;
- COBIT 5 DSS02.04, DSS02.07;
- ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5;
- NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4.

RS.AN-2 – O impacto do incidente deve ser avaliado

O **impacto dos incidentes** nos ativos do laboratório 10 deve ser **avaliado** no processo de **categorização dos incidentes** e permitirá avaliar a severidade de um determinado incidente.

O impacto de um incidente num ativo e na sua operacionalidade permitirá definir os **níveis de impacto de incidentes**, que são a base da definição de "*tempos de resposta*, *de resolução, níveis de alerta e prioridade*". (Centro Nacional de Cibersegurança, 2019)

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 DSS02.02;
- ISO/IEC 27001:2013 A.16.1.4, A.16.1.6;
- NIST SP 800-53 Rev. 4 CP-2, IR-4.

RS.AN-3 – Devem ser realizadas análises forenses

No processo de **resposta a incidentes**, deverá existir condições para que se possa efetuar análises forenses. Essas condições passam pela existência de **gestão e correlação de eventos** e ***software* de captura de dados** em bruto (discos, memórias e/ou pacotes de rede).

Devem ser adotados procedimentos que permitam a **identificação**, **recolha de registos/informação** e a **garantia da integridade** e **conservação** das evidências recolhidas.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

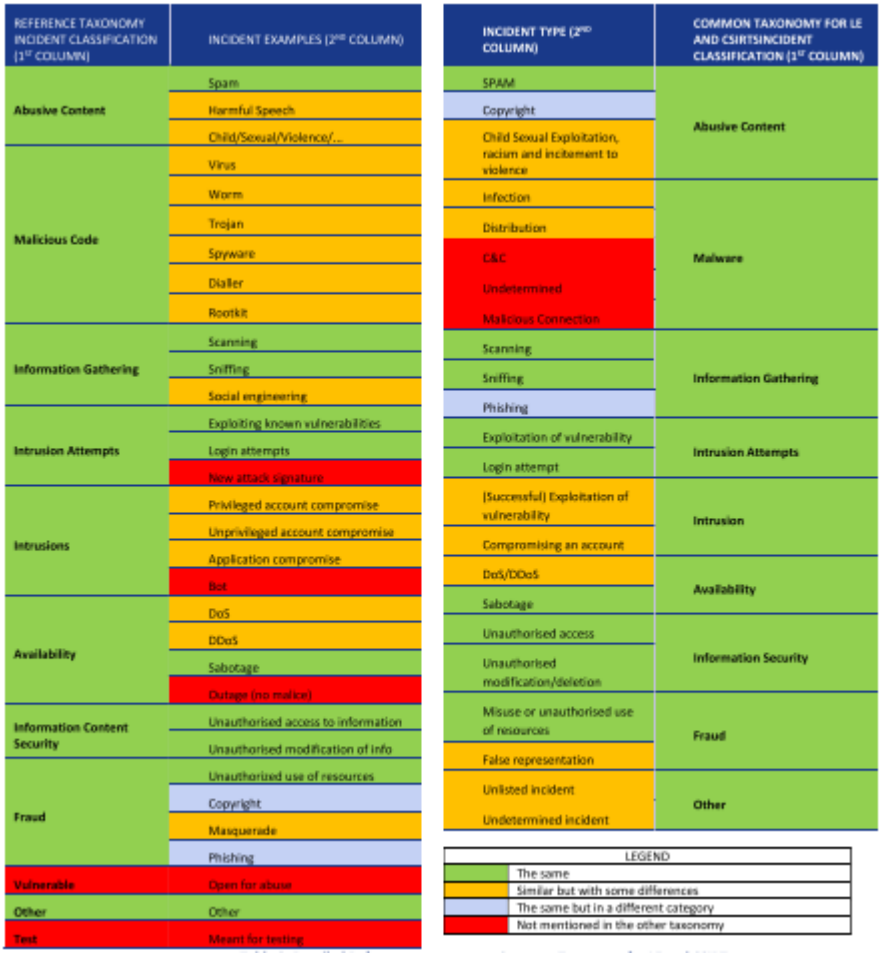
- COBIT 5 APO12.06, DSS03.02, DSS05.07;
- ISO/IEC 27001:2013 A.16.1.7;
- NIST SP 800-53 Rev. 4 AU-7, IR-4.

RS.AN-4 – Os incidentes devem ser categorizados de acordo com o plano de resposta

A categorização dos incidentes tem de ser efetuada com base nas regras definidas no **plano de resposta a incidentes** do laboratório 10. A categorização dos incidentes pode ser feita com base na proposta apresentada na **Taxonomia Nacional para a classificação de incidentes**.

Segundo ENISA, 2018, a criação da **lista de referência da taxonomia da classificação e incidentes** surgiu do facto de, anteriormente, as organizações criarem uma taxonomia de classificação correspondente às suas necessidades. Com o aumento da necessidade de troca de informações e relatórios de incidentes, foi sentida a necessidade de criar um padrão comum, de forma a ajudar as organizações e até mesmo ajudar as entidades com a criação da estratégia de cibersegurança da UE e a diretiva de segurança de redes e sistemas de informação (Comissão Europeia, 2016a).

A **Taxonomia Comum** para aplicação da lei (LE) e CSIRTs é uma adaptação da taxonomia CERT.PT, que também é uma adaptação da taxonomia e CSIRT.net mkVI.



REFERENCE TAXONOMY INCIDENT CLASSIFICATION (1ST COLUMN)	INCIDENT EXAMPLES (2ND COLUMN)
Abusive Content	Spam
	Harmful Speech
	Child/Sexual/Violence/...
Malicious Code	Virus
	Worm
	Trojan
	Spyware
	Dialler
	Rootkit
Information Gathering	Scanning
	Sniffing
	Social engineering
Intrusion Attempts	Exploiting known vulnerabilities
	Login attempts
	New attack signature
Intrusions	Privileged account compromise
	Unprivileged account compromise
	Application compromise
	Bot
Availability	DoS
	DDoS
	Sabotage
	Outage (no malice)
Information Content Security	Unauthorised access to information
	Unauthorised modification of info
Fraud	Unauthorized use of resources
	Copyright
	Masquerade
	Phishing
Vulnerable	Open for abuse
Other	Other
Test	Meant for testing

INCIDENT TYPE (2ND COLUMN)	COMMON TAXONOMY FOR LE AND CSIRTSINCIDENT CLASSIFICATION (1ST COLUMN)
SPAM	Abusive Content
Copyright	
Child Sexual Exploitation, racism and incitement to violence	
Infection	Malware
Distribution	
C&C	
Undetermined	
Malicious Connection	
Scanning	Information Gathering
Sniffing	
Phishing	
Exploitation of vulnerability	Intrusion Attempts
Login attempt	
(Successful) Exploitation of vulnerability	Intrusion
Compromising an account	
DoS/DDoS	Availability
Sabotage	
Unauthorised access	Information Security
Unauthorised modification/deletion	
Misuse or unauthorised use of resources	Fraud
False representation	
Unlisted incident	Other
Undetermined incident	

LEGEND	
	The same
	Similar but with some differences
	The same but in a different category
	Not mentioned in the other taxonomy

Figura 9 - Taxonomia de Referência detalhada vs Taxonomia Comum para LE e CSIRTs *(Comissão Europeia, 2016a)*

Na Figura 9 está representada a diferença entre a taxonomia de referência e a taxonomia comum para LE e CSIRTs. As diferenças mais salientes entre as duas são o facto de a taxonomia de referência se focar mais na especificação do *malware* e a taxonomia comum se focar mais na distinção entre infeção e distribuição.

A instituição deve criar a sua taxonomia de referência com a ajuda de ambas as taxonomias, pois estas vão ajudar a determinar que tipos de incidentes se adequam mais ao contexto do laboratório 10.

Taxonomia de Referância Lab10	Tipo de Incidente
Código Malicioso	Vírus
	Worm
	Trojan
	Spyware
	Dialer
	Rootkit
Roubo de Informação	*Scanning*
	Sniffing
	Phising
Tentativas de Intrusão	Exploração de Vulnerabilidades
	Tentativa de *Login*
Intrusão	Sucesso na exploração das vulnerabilidades
	Comprometimento das contas privilegiadas
	Comprometimento das contas não privilegiadas
Disponibilidade	*DoS/DDoS*
	Sabotagem
Segurança da Informação	Acessos não autorizados
	Modificação e remoção não autorizadas
Fraude	Uso indevido ou não autorizado de recursos
	Argumentos Inválidos
Outros	Incidentes não documentados
	Incidentes não determinados

Figura 10 - Taxonomia de Referência Lab10

Na Figura 10 está representada uma possível taxonomia de incidentes, adaptada ao contexto e ao funcionamento do laboratório 10. De salientar que esta taxonomia deve ser revista sempre que os registos na secção de "Outros" comecem a atingir um número considerável.

RS.AN-5 – A organização deve definir processos para receber, analisar e responder a vulnerabilidades provenientes de fontes internas e externas

O **processo de submissão de vulnerabilidades** deve conter metodologias formais de forma a que tanto fontes internas como externas, saibam como reportar o problema de forma consistente. A submissão dessas vulnerabilidades pode surgir de **testes internos**, **relatórios** ou **investigações de segurança**.

Esta **submissão de vulnerabilidades** deve ser **analisada/avaliada**, **tratada** e **respondida** de forma sistematizada, prevista no processo de resposta a vulnerabilidades anteriormente definido.

Este processo formal deve contemplar a **receção de alertas de segurança**, **recomendações**, **diretrizes** de fornecedores, fabricantes e entre outros.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 4, 19;
- COBIT 5 EDM03.02, DSS05.07;
- NIST SP 800-53 Rev. 4 SI-5, PM-15.

RS.MI – Mitigação

RS.MI-1 – Os incidentes devem ser contidos

Com o objetivo de conter os incidentes ocorridos de forma eficaz, é necessário a **criação/definição de processos/procedimentos para a resolução e tratamento dos incidentes**.

Relativamente à capacidade de investigação, de forma a saber em que direção se deve seguir, é necessário a **análise de *malware***, **análise** e **correlação** de **registos** ou até mesmo uma análise forense.

Após esta análise, é necessário fazer uma **sumarização das evidências** encontradas e **definir recomendações**, tais como (Centro Nacional de Cibersegurança, 2019):

- O que fazer em "***curto e longo prazo*** *para conter o* ***incidente*****"**, o mesmo deve ser **separado do resto do ambiente**;
- Verificar o que está disponível em **cópias de segurança** e se é possível ser restaurado;
- Que **credenciais** devem ser **atualizadas/alteradas** ou até mesmo os **mecanismos de autenticação reforçados**;
- As possíveis ligações de **rede/sessões** que devem ser **fraturadas;** e

- Que **sistemas** devem receber **atualizações** de segurança no imediato.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 19;
- COBIT 5 APO12.06;
- ISO/IEC 27001:2013 A.12.2.1, A.16.1.5;
- NIST SP 800-53 Rev. 4 IR-4.

RS.MI-2 – Os incidentes devem ser mitigados

A mitigação dos incidentes deve seguir **processos e procedimentos sistematizados** para a **resolução e tratamento** desses mesmos **incidentes**. Esses processos/procedimentos devem também verificar a mitigação completa dos incidentes. Para estas ações serem completadas, devem ser seguidos quatro passos: **contenção do incidente**, **redução do impacto do incidente**, **erradicação** e, por fim, **documentação**.

A **contenção do incidente** pode passar pelas seguintes ações: "***bloquear contas***, ***serviços e websites***, ***segregar redes ou contas de utilizadores***, ***suspender o acesso à internet, alterar palavras-passe***, ***fechar portos de comunicação***, ***desligar sistemas da rede de comunicações***". (Centro Nacional de Cibersegurança, 2019)

A **redução do impacto** pode passar pela aplicação de medidas de **disponibilização de novos servidores**, o **controlo da disponibilidade dos serviços**, isto é, criar mecanismos que permitam que o serviço não fique totalmente indisponível e que os utilizadores possam aceder a partes do mesmo até a situação esteja resolvida (degradação graciosa) ou encontrar **serviços** que possam, **temporariamente**, satisfazer as **necessidades dos utilizadores**.

A **erradicação do incidente** pode passar por **medidas de remoção do *malware*** usado no ataque, **atualização de segurança**, **restauração das cópias de segurança** necessárias e **melhoria das palavras-passe** e dos **fatores de autenticação**.

Por fim, deverão ser **documentadas** informações sobre **quais os sistemas que foram comprometidos com o ataque**, uma análise de **causa raiz** e qual a **informação perdida/exfiltrada**. (Centro Nacional de Cibersegurança, 2019)

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 4, 19;
- COBIT 5 APO12.06;
- ISO/IEC 27001:2013 A.12.2.1, A.16.1.5;
- NIST SP 800-53 Rev. 4 IR-4.

RS.MI-3 – As novas vulnerabilidades identificadas devem ser mitigadas ou documentadas como riscos aceites

As atividades previstas na gestão das vulnerabilidades preveem que as **novas vulnerabilidades** sejam **identificadas** e **avaliadas formalmente** e, por parte da Maiêutica, deve ser definido qual o **tratamento para cada uma dessas vulnerabilidades**.

Como já mencionado no **ID.GR-3**, cabe à instituição fazer algo para **remediar/corrigir as vulnerabilidades identificadas** ou **documentar formalmente a aceitação do risco** diretamente associado, com as devidas justificações do mesmo.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 4;
- COBIT 5 APO12.06;
- ISO/IEC 27001:2013 A.12.6.1;
- NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5.

RS.ME – Melhorias

RS.ME-1 – Os planos de resposta a incidentes devem incorporar as lições aprendidas

Após a finalização dos **incidentes**, é feita a análise dos mesmos **para identificar quais as lições a serem aprendidas**. Devem ser organizadas **sessões** com a **equipa responsável pelo processo de resposta a incidentes**, sendo que nessas sessões serão **analisados e documentados** os seguintes pontos: toda a **informação sobre o incidente**, o que **funcionou bem na resolução do mesmo** e o que é **preciso melhorar no plano de resposta**.

Esta pequena análise deverá levar a uma **implementação de um plano de melhoria**. Este plano pode ser constituído com **informação sobre as alterações** que podem ser feitas de forma a **melhorar a segurança**, **analisando as fragilidades** que foram exploradas, o que pode e/ou deve ser **executado de forma melhorada**, se há necessidade de **formação** para melhorar a capacidade de algum elemento da equipa de resposta e como se poderá garantir que não volta a acontecer.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 BAI01.13;
- ISO/IEC 27001:2013 A.16.1.6, Cláusula 10;
- NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8.

RS.ME-2 – As estratégias de resposta a incidentes devem ser atualizadas

Ao longo do tempo, podem existir mudanças que influenciem a atualização do plano de resposta a incidentes. Essas **mudanças** podem passar pelos **ativos**, **colaboradores**,

responsáveis pelos ativos, entre outros. Por este motivo, e pelo facto de que as ameaças e vulnerabilidades estão constantemente a alterar, o **plano de resposta** a incidentes deve ser **atualizado com bastante frequência**.

Com este processo e devido ao ambiente dinâmico que a Maiêutica e o laboratório 10 em que se encontram, deve ser **atualizada** com frequência a **lista das redes e sistemas de informação** que suportam os **serviços críticos**, a **lista de contactos internas** e com as **organizações externas** e a **resposta tática** a determinadas ameaças.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 BAI01.13, DSS04.08;
- ISO/IEC 27001:2013 A.16.1.6, Cláusula 10;
- NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8.

Recuperar

A medida de segurança Recuperar tem como principal objetivo definir e implementar medidas que permitem a identificação de incidentes, ou seja, eventos que tenham um efeito negativo na segurança das redes e sistemas de informação. Estas medidas têm como finalidade "*assegurar a resiliência da organização nas suas dimensões Pessoas, Processos e Tecnologia*." (Centro Nacional de Cibersegurança, 2019)

Esta medida de segurança é constituída por três categorias (**RC.PR**, **RC.ME** e **RC.CO**) e as subcategorias variam entre um mínimo de um e um máximo de dois.

RC.PR – Plano de Recuperação

RC.PR-1 – A organização deve seguir um plano de recuperação durante ou após um incidente

A **recuperação** após um incidente deve ser feita com base no **processo de recuperação de incidentes** criado pela instituição. O processo tem de garantir a co**rreta aplicação** de **recursos**, sejam **humanos**, **tecnológicos** e/ou **processuais**. As atividades de **recuperação**, o seu **rigor**, **âmbito**, **aplicabilidade** e **resultados** devem ser consistentes e transversais a todos os incidentes.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- CIS CSC 10;
- COBIT 5 APO12.06, DSS02.05, DSS03.04;
- ISO/IEC 27001:2013 A.16.1.5;
- NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8.

RC.ME – Melhorias

RC.ME-1 – Os planos de recuperação devem incorporar as lições aprendidas

As **lições aprendidas** com a **implementação do plano de recuperação** devem resultar em **ações** que ajudarão na **implementação do plano de melhoria**. Devem ser feitas **avaliações da eficácia** dos **planos de recuperação** em vigor, a iden**tificação das fragilidades** dos mesmos e das oportunidades de melhoria que surgiram e, por fim, a devida **atualização do plano** com base nas melhorias identificadas.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 APO12.06, BAI05.07, DSS04.08;
- ISO/IEC 27001:2013 A.16.1.6, Cláusula 10;
- NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8.

RC.ME-2 – As estratégias de recuperação devem ser continuamente revistas e atualizadas

Tanto a Maiêutica como o laboratório 10 têm um funcionamento dinâmico no que toca a ativos e aos seus responsáveis (recursos humanos). Os **planos de recuperação** e as suas **estratégias** devem ser **atualizados seguindo as necessidades de atualização** de dados de **contactos**, **ativos** e **prioridades**.

Deve ser **atualizada** com frequência a "***lista das redes e sistemas de informação*** *que suportam os serviços críticos, as* ***técnicas de recuperação dos sistemas de informação*** *e as* ***listas dos contactos dos responsáveis***" **técnicos e funcionais**. (Centro Nacional de Cibersegurança, 2019)

Estes **planos de recuperação** devem sempre ter associado um **documento de suporte** e um **registo das atualizações** feitas a estes mesmos planos de recuperação de incidentes.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 APO12.06, BAI07.08;
- ISO/IEC 27001:2013 A.16.1.6, Cláusula 10;
- NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8.

RC.CO – Comunicações

RC.CO-1 – A organização deve implementar um plano de comunicação

A instituição deve ter a capacidade de **detetar** o que é relevante ou não ser **compartilhado** e o **fluxo de comunicação** deve ser **controlado** para que não haja oportunidades de minimização da credibilidade e reputação da informação e da instituição.

Tal como anteriormente citado nas subcategorias **DE.PD-4** e **RS.CO-4**, o plano de comunicação definido deverá identificar:

"*1) O que comunicar: Que conteúdo (por exemplo: a forma adequada como foi tratado um incidente de cibersegurança);*

2) Que mensagem: Forma e formato, que tipo de meio será usado, desde pequenos textos a imagens, metáforas, vídeos, entre outros;

3) Quem deve comunicar: Deve ser nomeado um responsável que tem a autoridade e autonomia para comunicar, particularmente com organizações externas;

4) A quem comunicar: Destinatários da comunicação;

5) Como comunicar: Que canais devem ser usados para obter a melhor eficácia na difusão da mensagem (por exemplo: mensagens de correio eletrónico, protetores de ecrã);

6) Quando comunicar: A comunicação deve ser regularmente exercitada em condições comuns (por exemplo: divulgação da política de segurança da informação), mas poderá ter frequências e modos de atuação muito diferentes em contexto de incidente." (Centro Nacional de Cibersegurança, 2019)

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 EDM03.02;
- ISO/IEC 27001:2013 A.6.1.4, Cláusula 7.4.

RC.CO-2 – As atividades de recuperação devem ser comunicadas às partes interessadas, internas e externas, bem como às equipas executivas e de gestão

A instituição deve definir uma **estratégia de comunicação** com as partes interessadas, tanto **internas** como **externas**, com base no plano de comunicação previamente criado.

Nesta subcategoria, deverão ser identificados: o procedimento de escalonamento de incidentes, a tipificação atribuída a incidentes e quais devem motivar o contacto com as partes interessadas externas, o plano de comunicação a estabelecer e, por fim, quais as partes interessadas que deverão ser contactadas.

Referências Normativas (Centro Nacional de Cibersegurança, 2019)**:**

- COBIT 5 APO12.06;
- ISO/IEC 27001:2013 Cláusula 7.4;
- NIST SP 800-53 Rev. 4 CP-2, IR-4.

Conclusão

O aumento significativo de dispositivos ligados entre si pela *Internet* fez com que as organizações tivessem de ser consciencializadas de que a segurança das redes e dos sistemas de informação nunca foi tão importante.

O Quadro Nacional de Referência para a Cibersegurança tem como função apresentar às organizações os requisitos mínimos a serem cumpridos por parte da mesma de forma a reduzir o risco associado à sua segurança digital. A análise do documento por parte da organização deverá ser de espírito crítico pois as organizações encontram-se, naturalmente, em diferentes níveis de maturidade. No relatório em causa, foi feita uma adaptação para o contexto do Laboratório 10, que não é uma organização, mas depende sempre da Maiêutica.

As medidas de segurança apresentadas no QNRCS são cinco: Identificar, Proteger, Detetar, Responder e Recuperar. O documento apresentado aborda as categorias e subcategorias do QNRCS no contexto do Laboratório 10 e às necessidades apresentadas pelos seus diferentes utilizadores.

A medida de segurança Identificar, tal como o próprio nome indica, é uma medida que prevê que a instituição identifique tudo o que é importante para saber como executar as seguintes medidas de segurança. A identificação começa pelos equipamentos, as plataformas, as redes e os fluxos de dados do laboratório 10. Após isso, é importante identificar quais os fornecedores, os ativos críticos, os cenários de crise, as vulnerabilidades e as ameaças. Por fim, definir quais os responsáveis pela gestão do risco e do tratamento desses riscos e qual a tolerância aos mesmos.

Na medida de segurança Proteger, o objetivo é a instituição adotar medidas de proteção do laboratório 10, como um todo. É importante o melhoramento de sistemas de gestão de identidades, autenticação e controlos de acesso. Para além disso, é fundamental sensibilizar e formar os diversos colaboradores de quais as suas diferentes responsabilidades perante o laboratório 10. A instituição terá de verificar junto dos fornecedores se os contratos com os mesmos permitem a manutenção e recuperação dos equipamentos no caso de danos.

A medida de segurança Detetar permite à instituição a implementação de métodos de deteção de eventos. Métodos esses que podem ser de monitorização das redes e sistemas de informação do laboratório 10 e aplicáveis em ambientes físicos e lógicos. A deteção de eventos leva à coleta e correlação dos mesmos e, de seguida, à medição do impacto dos mesmos e qual a possibilidade de se tornarem incidentes.

Na medida de segurança Responder, a instituição terá de definir planos de resposta a eventos que tenham sido detetados na medida de segurança anterior. Planos estes constituídos por um processo de resolução de incidentes, onde deverão constatar os responsáveis pelo tratamento de incidentes, que farão a alocação dos recursos durante o processo de resolução. Após os incidentes é importante identificar quais os impactos desses mesmos incidentes e categorizá-los. Por fim, devem ser identificadas novas vulnerabilidades e, posteriormente, escolher qual a ação que executará, ou não, sobre os riscos que as mesmas implicam.

A quinta, e última medida de segurança, Recuperar leva a instituição à definição e execução do plano de recuperação de incidentes, sendo que a implementação pode ser durante ou após os incidentes. Após a recuperação, é importante a execução do plano de melhorias onde são executadas ações com base nas conclusões tiradas do impacto desses mesmos incidentes. Este plano, tal como todos os mencionados neste documento, devem ser revistos com regularidade. Ao longo de todo o documento foi várias vezes mencionada a importância da existência de um plano de comunicação de vulnerabilidades e incidentes.

Referências

1 Channel 5V Relay Shield Module. (n.d.). Retrieved January 15, 2021, from https://www.ptrobotics.com/modulos-de-reles/3635-1-channel-5v-relay-shield-module.html?gclid=CjwKCAiAl4WABhAJEiwATUnEF68M8JqyrL17neV19BDAxC54ru8Uw8g7U3lmv3031JJrc6I7SpKfYBoCebIQAvD_BwE

Ada, Lady. (2020). Adafruit Learning System: PIR Motion Sensor. In *Adafruit Learning System* (pp. 1–28). https://cdn-learn.adafruit.com/downloads/pdf/pir-passive-infrared-proximity-motion-sensor.pdf?timestamp=1585441256

Al-falahy, N., & Alani, O. Y. (2017). *Technologies for 5G Networks : Challenges and Opportunities*.

Al-kahtani, M. A., & Sandhu, R. (2002). *A Model for Attribute-Based User-Role Assignment*.

Aosong Electronics. (2010). Temperature and Humidity Module, AM1001. *Datasheet*, 9.

Arduino - Setting up an Arduino on a breadboard. (n.d.). Retrieved January 15, 2021, from https://www.arduino.cc/en/main/standalone

Arduino Nano | Arduino Official Store. (n.d.). Retrieved January 15, 2021, from https://store.arduino.cc/arduino-nano

Ashraf, Q. M., Habaebi, M. H., Islam, M. R., & Khan, S. (2016). Device discovery and configuration scheme for Internet of Things. *2016 International Conference on Intelligent Systems Engineering, ICISE 2016*, 38–43. https://doi.org/10.1109/INTELSE.2016.7475159

Assembleia da República. (2018a). *Lei 46/2018, 2018-08-13 - DRE*. https://dre.pt/home/-/dre/116029384/details/maximized

Assembleia da República. (2018b). *Política Geral de Segurança da Informação da Assembleia da República*. 1–5.

Barbosa Cabral, J. L. (2017). *Massive MIMO*. ISCTE-IUL.

Bastos, A. V., & Cecílio, D. (2017). *Minicurso - Comunicação D2D para 5G de Arquiteturas de Redes Celulares : Da Teoria à Prática* (Issues 1–30). https://doi.org/10.13140/RG.2.2.18432.12807

Beatrys Ruiz, L., A. Correia, L. H., M. Vieira, L. F., F. Macedo, D., F. Nakamura, E., M. S. Figueiredo, C., M. Vieira, M. A., Habib Bechelane, E., Camara, D., A. F. Loureiro, A., S. Nogueira, J. M., C. da Silva Jr., D., & O. Fernandes, A. (2004). Arquiteturas para Redes de Sensores sem Fio. In *Arquiteturas para Redes de Sensores sem Fio*.

Breadboard Power Supply Module 3.3V/5V. (n.d.). Retrieved January 15, 2021, from https://www.ptrobotics.com/alimentacao/5924-breadboard-power-supply-module-33v-5v.html?gclid=CjwKCAiAl4WABhAJEiwATUnEF5G9RMJfNchWOLKHdrOkpKX5GpvympvLEjphNtAjuFstalzapx466hoCOEkQAvD_BwE

Centro Nacional de Cibersegurança. (2019). *Quadro Nacional de Referência para a Cibersegurança*. https://www.cncs.gov.pt/content/files/cncs_qnrcs_2019.pdf

Chess, D. M., & Kephart, J. O. (2003). The Vision of Autonomic Computing. *Computer*, *36*(January), 41–50. https://doi.org/10.1046/j.1365-2745.2002.00730.x

Chung, A., Dawda, S., Hussain, A., Shaikh, S. A., & Carr, M. (2014). Cybersecurity: Policy. In *Encyclopedia of Security and Emergency Management* (Vol. 1, pp. 1–15). https://doi.org/10.1007/978-3-319-69891-5_20-1

Comissão Europeia. (2016a). DIRETIVA (UE) 2016/1148 DO PARLAMENTO EUROPEU

E DO CONSELHO de 6 de julho de 2016. *Official Journal of the European Union*, *2014*(2), 1–30. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148

Comissão Europeia. (2016b). *L_2016119PT.01000101.xml*. Jornal Oficial Da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679

Conference, I., & Systems, I. (2018). *Automatic Integration of IoT Devices* (Issue 351).

DHT11 Sensor Pinout, Features, Equivalents & Datasheet. (n.d.). Retrieved January 15, 2021, from https://components101.com/dht11-temperature-sensor

diagrams.net. (n.d.). Retrieved January 20, 2021, from https://app.diagrams.net/

Display LCD 16x2 I2C com fundo azul. (n.d.). Retrieved January 15, 2021, from https://www.electrofun.pt/display/display-lcd-16x2

DSSS - Direct Sequence Spread Spectrum - YouTube. (n.d.). Retrieved January 20, 2020, from https://www.youtube.com/watch?v=-1mxYWvfVWQ&list=WL&index=13&t=0s

ENISA. (2018). Reference Incident Classification Taxonomy Task Force Status and Way Forward. In *European Union Agency For Network and Information Security* (Issue January, p. 20).

FE & MO TECHNOLOGY S.L.U. (n.d.). Retrieved January 15, 2021, from https://www.moveteck.com/producto/0751572/GT882-NE-Cargador-Universal-BM-24W-con-1USB-6W%2C-3V-12V-2A-con-6-tips

FHSS - Frequency Hopping Spread Spectrum - YouTube. (n.d.). Retrieved January 20, 2020,

from https://www.youtube.com/watch?v=CkhA7s5GIGc&list=WL&index=12&t=271s

Gil, J. M. V. S. (2012). *Monitorização, Alarmística e Gestão de Redes*. Instituto Politécnico de Leiria.

Glória, A., Cercas, F., & Souto, N. (2017). Design and implementation of an IoT gateway to create smart environments. In *Procedia Computer Science*. https://doi.org/10.1016/j.procs.2017.05.343

Guedes, G. T. A. (2018). *UML 2 - Uma Abordagem Prática - Gilleanes T. A. Guedes - Google Livros* (Novatec (Ed.); 3ª). https://books.google.com.br/books?hl=pt-PT&lr=&id=mJxMDwAAQBAJ&oi=fnd&pg=PA2&dq=diagramas+da+uml&ots=x9sQPiXOl0&sig=_sJSXHEV6xFn2FqI8WfyhC5uuvs#v=onepage&q=diagramas da uml&f=false

H. Mahmoud, Q. (2007). *Congnitive Networks - Towards Self-Aware Netowrks*.

Haartsen, J. (1998). Bluetooth - the universal radio interface for ad hoc, wireless connectivity. *Ericsson Review (English Edition)*, *75*(3), 110–117.

Handsontec. (2017). Handson Technology. *Hanson Technology*, 1–22. http://www.handsontec.com/pdf_learn/esp8266-V10.pdf

IEC. (2016). *ISO/IEC 20922:2016 | IEC Webstore*. https://webstore.iec.ch/publication/25096

IEEE. (2019). *P802.15.4-REVd/D04, Oct 2019 - IEEE Draft Standard for Low-Rate Wireless Networks (WPANs) - IEEE Standard*. https://ieeexplore.ieee.org/document/8935588?denied=

IREO - Distribuidor de Soluções TI. (2019). *ManageEngine*. https://www.ireo.com/pt/fabricantes-e-produtos/manageengine

ISO/IEC. (2012). *ISO/IEC 27032:2012(en), Information technology — Security techniques — Guidelines for cybersecurity*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

ISO/IEC. (2018a). *ISO/IEC 27005:2018(en), Information technology — Security techniques — Information security risk management*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en

ISO/IEC. (2018b). *Risk management ISO 31000*.

Jaouhari, S. E. L., Palacios-Garcia, E. J., Anvari-Moghaddam, A., & Bouabdallah, A. (2019). Integrated management of energy, wellbeing and health in the next generation of smart homes. In *Sensors (Switzerland)* (Vol. 19, Issue 3). https://doi.org/10.3390/s19030481

Keeler, J. (2004). MFRC522: Contactless Reader IC. *Understanding NMR Spectroscopy*, *May*, 1-1-1–3.

Khan, P. M., & Quraishi, K. A. (2014). Impact of RACI on delivery and outcome of software development projects. *International Conference on Advanced Computing and Communication Technologies, ACCT*, 177–184. https://doi.org/10.1109/ACCT.2014.66

Kim, E., Kaspar, D., Gomez, C., & Bormann, C. (2012). Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing. In *RFC6606*.

Lampson, B. W. (1974). Protection. *Information Sciences*, 18–24.

Liikanen, J., Stoneman, P., & Toivanen, O. (2004). Intergenerational effects in the diffusion of new technology: The case of mobile phones. *International Journal of Industrial Organization*, *22*(8–9), 1137–1154. https://doi.org/10.1016/j.ijindorg.2004.05.006

ManageEngine NCM. (n.d.). *Schedule network device configuration backup*. Retrieved November 17, 2019, from https://www.manageengine.com/network-configuration-manager/scheduling-configuration-tasks.html

Marques, A. F. C. (2015). *Desenho e Implementação de uma Plataforma Integrada para Monitorização e Gestão de uma Rede de um Departamento da UMa* [Universidade da Madeira]. https://digituma.uma.pt/bitstream/10400.13/1246/1/MestradoAndreiaMarques.pdf

Microchip Technology Inc. (2006). Data Sheet Stand-Alone Ethernet Controller with SPI Interface. *Technology*.

Módulo Leitor RFID RC522 Arduino. (n.d.). Retrieved January 15, 2021, from https://www.electrofun.pt/comunicacao/leitor-rfid-arduino

Mukherjee, S., & Biswas, G. P. (2018). Networking for IoT and applications using existing communication technology. *Egyptian Informatics Journal*, *19*(2), 107–127. https://doi.org/10.1016/j.eij.2017.11.002

Myers, A. C., & Liskov, B. (1997). *A decentralized model for information flow control*. https://doi.org/10.1145/268998.266669

NIST. (2018). Framework for improving critical infrastructure cybersecurity. *Proceedings of the Annual ISA Analysis Division Symposium*, *535*, 9–25.

Office of the Law Revision Counsel of the U.S. House of Representatives. (1968). *44 U.S.*

Code CHAPTER 35— COORDINATION OF FEDERAL INFORMATION POLICY Subchapter II § 3552. Definitions. 3553. https://www.law.cornell.edu/uscode/text/44/3552

Olimex. (2013). Tecnical Data Mq-135 Gas Sensor. In *Hanwei Electron* (Vol. 1, pp. 3–4).

P. Pfleeger, C., Lawrence Pfleeger, S., & Margulies, J. (2015). *Security in Computing*.

Patino, S., Solis, E. F., Yoo, S. G., & Arroyo, R. (2018). ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO/IEC 27005. *2018 5th International Conference on EDemocracy and EGovernment, ICEDEG 2018*, 75–82. https://doi.org/10.1109/ICEDEG.2018.8372361

Patrick Kinney. (2003). ZigBee Technology : Wireless Control that Simply Works. *Communications Design Conference, October*, 1–20.

Paulsen, C. Toth, P. (2016). Small Business Information Security: The Fundamentals Small Business. In *National Institute of Standards and Technology Interagency Report* (Vol. 7621, p. 54). https://doi.org/10.6028/NIST.IR.7621r1

Philips. (2002). *Data Sheet PCF8574* (pp. 0–24). http://www.papersearch.net/view/detail.asp?detail_key=10000715

Pires, J. (2018). *Gestão técnica e operacional da rede metropolitana da Associação Porto Digital*.

Ruiz, L. B. (2003). *Maná: uma arquitetura para gerenciamento de redes de sensores sem fio*. http://www2.dcc.ufmg.br/~linnyer/TeseMANNA.pdf%5Cnhttp://www2.dcc.ufmg.br/%7B~%7Dlinnyer/TeseMANNA.pdf

Sá Silva, J., Mendão Silva, R., & Boavida, F. (2016). *Redes de Sensores sem Fios - Informática - Redes & Comunicações - FCA*. 2016. https://www.fca.pt/pt/catalogo/informatica/redes-comunicacoes/redes-de-sensores-sem-fios/

Saha, S., & Majumdar, A. (2017). Data centre temperature monitoring with ESP8266 based Wireless Sensor Network and cloud based dashboard with real time alert system. *Proceedings of 2nd International Conference on 2017 Devices for Integrated Circuit, DevIC 2017*, 307–310. https://doi.org/10.1109/DEVIC.2017.8073958

Saleiro, M., & Ey, E. (2009). *ZigBee uma abordagem prática*.

Sensor de Gases MQ-135. (n.d.). Retrieved January 17, 2021, from https://www.botnroll.com/pt/biometricos/2195-sensor-de-gases-mq-135.html

Sensor de Som c/ saída Analógica e Digital. (n.d.). Retrieved January 15, 2021, from https://www.botnroll.com/pt/som/2162-sensor-de-som-c-saida-analogica-e-digital.html

Sensor PIR / Sensor Movimento para Arduino. (n.d.). Retrieved January 15, 2021, from https://www.electrofun.pt/sensores-arduino/sensor-movimento-pir-arduino

Shelby, Z., & Bormann, C. (2011). The Wireless Embedded Internet. In *Annals of CASE* (Vol. 43). http://www.sase.com.ar/2011/files/2011/02/59-Wireless_Embedded_Internet_6LowPan.pdf

SHENZHEN RUITE ELECTRONIC CO., L. (n.d.). *RT162-7* (p. 1).

SolarWinds. (2019). *Software de gerenciamento de TI e ferramentas de monitoramento*.

Souza, L. De, Rosa, P., Barcelos, R. G., Pereira, Y., & Real, Y. (2017). *Aplicações do 5G em*

Internet das Coisas (IoT).

Systems, C. on N. S. (2015). *Committee on National Security Systems (CNSS) Glossary* (Issue 4009, pp. 1–165). https://doi.org/10.1201/9780203888933.ch13

Tahir, M., Mamoon Ashraf, Q., & Dabbagh, M. (2019). Towards enabling autonomic computing in IoT ecosystem. *Proceedings - IEEE 17th International Conference on Dependable, Autonomic and Secure Computing, IEEE 17th International Conference on Pervasive Intelligence and Computing, IEEE 5th International Conference on Cloud and Big Data Computing, 4th Cyber Scienc, August*, 646–651. https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00122

Teixeira De Gouveia, B. A. (2009). *Dispositivos de Monitorização e Controlo automático de fatores climáticos em Museus*. Universidade da Madeira.

Thomas, P., & Kumar, J. P. (2019). Cloud Based Dynamic Energy Management in Power System Using Message Queuing Telemetry Transport (MQTT) Protocol. *Proceedings of the 3rd International Conference on Electronics and Communication and Aerospace Technology, ICECA 2019*, 1301–1305. https://doi.org/10.1109/ICECA.2019.8821818

Ubidots. (2020). *IoT platform | Internet of Things*. https://ubidots.com/

VMA303: MÓDULO DE SENSOR DE HUMIDADE DO SOLO & SENSOR DE NÍVEL DE ÁGUA – Velleman – Wholesaler and developer of electronics. (n.d.). Retrieved January 15, 2021, from https://www.velleman.eu/products/view?id=435520&country=be&lang=pt

Wheeler, A. (2007). Commercial applications of wireless sensor networks using ZigBee. *IEEE Communications Magazine*, *45*(4), 70–77.

https://doi.org/10.1109/MCOM.2007.343615

Xu, K., Wan, Y., & Xue, G. (2019). Powering Smart Homes with Information-Centric Networking. *IEEE Communications Magazine*, *57*(6), 40–46. https://doi.org/10.1109/MCOM.2019.1800732

Yassein, M. B., Mardini, W., & Khalil, A. (2016). Smart homes automation using Z-wave protocol. *Proceedings - 2016 International Conference on Engineering and MIS, ICEMIS 2016*, 1–6. https://doi.org/10.1109/ICEMIS.2016.7745306

Yuan, M. (2017). *Conhecendo o MQTT*. https://www.ibm.com/developerworks/br/library/iot-mqtt-why-good-for-iot/index.html

Z-wave. (2019). *Introduction to Z-Wave - An Introductory Guide to Z-Wave Technology*.

Z-Wave. (2019). *Introduction to Z-Wave - An Introdutory Guide to Z-Wave Technology*.

Zheng, J., Simplot-ryl, D., Bisdikian, C., & Mouftah, H. T. (2011). The internet of things [Guest Editorial]. In *IEEE Communications Magazine* (Vol. 49, Issue November). IEEE. https://doi.org/10.1109/MCOM.2011.6069706